

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF NEW YORK

MATTHEW FERRO, et al.,

Plaintiffs,

v.

EXCELLUS HEALTH PLAIN, INC., et al.,

Defendants.

DECISION AND ORDER

6:15-CV-06569 EAW

INTRODUCTION

Those who are entrusted with details about an individual's health care should guard against even the inadvertent disclosure of that confidential information. Those duties were allegedly breached in this case when hackers secured access to confidential health care information through a cyberattack. Nonetheless, while legal remedies may be pursued by those who were injured, the law only allows for the pursuit of plausible claims—and only by those who have standing based on an alleged legally compensable injury. Not all parties or all claims in this case meet that standard.

This case arises out of a data breach involving Excellus Health Plan, Inc. ("Excellus"), a healthcare provider. Plaintiffs, who allege various claims and injuries arising from the data breach, bring this putative class action against the following eight defendants: Excellus, Lifetime Healthcare, Inc. ("Lifetime"), Lifetime Benefit Solutions, Inc., Genesee Region Home Care Association, Inc. d/b/a Lifetime Care, Genesee Valley Group Health Association d/b/a Lifetime Health Medical Group, MedAmerica, Inc.,

Univera Healthcare, and Blue Cross and Blue Shield Association (“BCBSA”).¹ In their Consolidated Master Complaint (“CMC”), Plaintiffs assert claims under various federal and state laws and seek, *inter alia*, class certification, injunctive relief, and damages. (Dkt. 99).

Presently before the Court are two motions to dismiss Plaintiffs’ CMC. (Dkt. 107; Dkt. 111). The Excellus Defendants and BCBSA—i.e., all Defendants—move to dismiss the CMC pursuant to Federal Rules of Civil Procedure 12(b)(1) and 12(b)(6), on the basis that the Court lacks jurisdiction because Plaintiffs lack standing to sue, and that Plaintiffs have failed to state a claim. (Dkt. 107-1 (“Excellus Mot.”)); (Dkt. 111-1 (“BCBSA Mot.)). For the reasons that follow, the Court grants in part and denies in part both motions.

BACKGROUND

I. Factual Background

The following factual allegations are drawn from Plaintiffs’ CMC.

A. The Parties

Excellus is “the primary healthcare provider in Upstate New York” and a licensee of BCBSA. (CMC at ¶ 37). Excellus is a subsidiary of Lifetime and a parent company to all other defendants, except Lifetime and BCBSA. (*Id.* at ¶ 40). Lifetime is “the parent and/or holding company of a \$6.6 billion family of companies, known as the Lifetime Healthcare Companies, that finances and delivers health care in New York State, as well

¹ The Court will refer to all defendants, including BCBSA, collectively as “Defendants.” The Court will refer to all defendants but BCBSA collectively as the “Excellus Defendants.”

as long-term care nationwide.” (*Id.* at ¶ 42). The following five defendants are affiliate companies of the Lifetime Healthcare Companies, and they are owned and controlled by Lifetime and Excellus: (1) Lifetime Benefit Solutions, Inc.; (2) Genesee Region Home Care Association, Inc. d/b/a Lifetime Care; (3) Genesee Valley Group Health Association d/b/a Lifetime Health Medical Group; (4) MedAmerica, Inc.; and (5) Univera Healthcare. (*Id.* at ¶¶ 45-49). The final defendant, BCBSA, “is a federation of 36 health insurance organizations and companies that provides health insurance to over 106 million individuals.” (*Id.* at ¶ 50). Excellus “cooperates with BCBSA and other independent Blue Cross Blue Shield . . . licensees to participate in the BlueCard program. Under the BlueCard program, members of one BCBS licensee may access another BCBS licensee’s provider networks and discounts.” (*Id.* at ¶ 55).

Plaintiffs allege three different types of classes. First, Plaintiffs allege “separate statewide classes for the states of California, Florida, Indiana, North Carolina, New Jersey, New York, and Pennsylvania,” defined as “[a]ll citizens of [name of state] whose [personally identifiable information (“PII”)] or [protected health information (“PHI”)] was compromised by the Excellus data breach” (“Statewide Classes”). (*Id.* at 64). Second, Plaintiffs allege a federal employee class, defined as “[a]ll enrollees in the Federal Employee Health Benefits Plan whose Personal Information was compromised by the Excellus data breach” (“Federal Employee Class”). (*Id.* at 65). Third, Plaintiffs allege a healthcare provider class, defined as “[a]ll healthcare providers and/or medical professionals who submitted PII directly or indirectly to Defendants and whose PII was compromised by the Excellus data breach” (“Healthcare Provider Class”). (*Id.* at 66).

B. The Data Breach

On December 23, 2013, hackers gained access to Excellus's computer network systems, which stored the personal information belonging to millions of individuals. (*Id.* at ¶¶ 52, 131, 133). During this data breach, the hackers had access to individuals' names, dates of birth, social security numbers, mailing addresses, telephone numbers, member identification numbers, financial payment information (including credit card numbers), and medical insurance claims information. (*Id.* at ¶¶ 1-3, 52, 134). The hackers also had access to healthcare providers' personal information, including medical licenses. (*Id.* at ¶ 135). The breach continued for 20 months, until at least August 18, 2014; however, the hackers may have had access to the systems more recently, on May 11, 2015. (*Id.* at ¶ 133).

"In the wake of other high-profile healthcare data breaches . . . , Defendants hired cybersecurity company Mandiant to forensically assess their systems." (*Id.* at ¶ 132). On August 4, 2015, Mandiant's analysis revealed malware on Defendants' systems. (*Id.*) On September 9, 2015, Defendants publicly announced that the breach had occurred and that it affected 10 to 10.5 million people, including past and current Excellus policyholders, as well as those who are insured by or receive healthcare services from Defendants' affiliates. (*Id.* at ¶ 138). According to that announcement, Mandiant's investigation did not determine that any personal information was removed from Excellus's systems, and Excellus had no evidence that the personal information was used inappropriately. (Dkt. 107-3, Ex. A). Defendants offered two years of free credit monitoring to adult victims of the breach. (CMC at ¶ 138).

Plaintiffs allege that Defendants had reason to know that their data security was inadequate both before the data breach started and after it was discovered by Defendants. (*Id.* at ¶¶ 114, 120). For example, in May 2012, the Department of Health and Human Services' Office for Civil Rights hired KPMG to conduct an audit of Univera (a Defendant and Lifetime affiliate company) in order to review its compliance with the Privacy, Security, and Breach Notification Rules of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"). (*Id.* at ¶ 115). The audit revealed, *inter alia*, that Univera's "Risk Assessment Policies & Procedures failed to identify the risks and vulnerabilities to the confidentiality, integrity, and availability of electronic PHI." (*Id.* at ¶ 117). As another example, in April 2014, the FBI Cyber Division "issued a 'Private Industry Notification' that explained how 'the health care industry is not technically prepared to combat against cyber criminals' basic cyber intrusion tactics, techniques and procedures (TTPs), much less against more advanced persistent threats (APTs). The health care industry is not as resilient to cyber intrusions compared to the financial and retail sectors, therefore the possibility of increased cyber intrusions is likely.'" (*Id.* at ¶ 123). This information, along with other data breaches in the health care industry, allegedly "put Defendants on notice that healthcare and health insurance companies were a target of cyberattack, and that these companies had an obligation to implement reasonable safeguards to keep pace. Defendants, quite simply, failed to heed the clear and unequivocal warning." (*Id.* at 129).

C. Plaintiffs' Alleged Injuries

Plaintiffs allege that the data breach caused them various types of injuries, both present and future. The following present injuries from the breach are alleged in the CMC. Four plaintiffs allege that false tax returns were filed in their names using their personal information, or that their personal information was accessed through the IRS portal. (*Id.* at ¶¶ 12, 19-20, 24, 29). Three plaintiffs allege that they are the victims of identity theft. (*Id.* at ¶¶ 18, 21, 22). Twelve plaintiffs have experienced fraudulent credit or debit card charges. (*Id.* at ¶¶ 21-28, 31-32, 34-35). Five plaintiffs allege that they spent money in order to remediate the breach or protect from future identity theft; this included purchasing additional credit monitoring services. (*Id.* at ¶¶ 20-23, 34). Three plaintiffs had delays in the receipt of their tax returns. (*Id.* at ¶¶ 19-20, 29). All plaintiffs spent time and effort to freeze their credit, place fraud alerts on their accounts, monitor credit reports and bank statements, and/or report identity theft to the relevant authorities. (*Id.* at ¶¶ 17-35). All plaintiffs allege anxiety and fear of identity theft as a result of the data breach. (*Id.* at ¶ 12). Plaintiffs also allege a risk of future, certainly impending harm as a result of the breach. (*See, e.g., id.* at ¶¶ 13, 19-35).

The Excellus Defendants differentiate the alleged injuries on the basis that four plaintiffs do not allege any specific instances in which their personal information was misused (*id.* at ¶¶ 17, 30, 33, 36), while the remaining sixteen plaintiffs allege some type of misuse of their personal information (*id.* at ¶¶ 18-29, 31-32, 34-35).

D. Plaintiffs' Causes of Action

Based on their factual allegations, Plaintiffs allege ten causes of action, as follows: (1) negligence; (2) negligence *per se*; (3) breach of contract; (4) breach of the implied covenant of good faith and fair dealing; (5) third-party beneficiary breach of contract for the Federal Employee Class; (6) negligent misrepresentation; (7) unjust enrichment; (8) violations of state consumer protection laws; (9) violation of the California Customer Records Act, Cal. Civ. Code § 1798.80; and (10) violations of state insurance personal privacy statutes.

II. Procedural History

Following the data breach, several potential victims filed lawsuits alleging various resulting injuries. (Dkt. 9-2 at 3). The earliest of such lawsuits was filed on September 18, 2015. (Dkt. 1). On November 5, 2015, the Court issued an order consolidating additional lawsuits, pursuant to Federal Rule of Civil Procedure 42(a)(2), and transferred the case to the undersigned. (Dkt. 27 at 4-5). On November 10, 2015, the Court entered an order directing that any subsequently-filed lawsuit arising out of the same facts or involving the same claims be consolidated into the lead action. (Dkt. 28). On January 25, 2016, the Court appointed interim lead counsel and directed Plaintiffs to file a consolidated master complaint. (Dkt. 80).

On April 15, 2016, Plaintiffs—twenty in all, from seven different states—filed the CMC. (Dkt. 99). On May 31, 2016, the Excellus Defendants filed a motion to dismiss. (Dkt. 107). On June 17, 2016, BCBSA filed a motion to dismiss. (Dkt. 111). Plaintiffs responded in opposition to the Excellus Defendants' motion to dismiss on July 7, 2016

(Dkt. 122-3 (“Pl. Excellus Opp.”)), and to BCBSA’s motion to dismiss on July 14, 2016 (Dkt. 129 (“Pl. BCBSA Opp.”)). On August 8, 2016, the Excellus Defendants and BCBSA each filed a reply in further support of their respective motions to dismiss. (Dkt. 133 (“Excellus Reply”); Dkt. 134 (“BCBSA Reply”)). Oral argument was held before the undersigned on September 8, 2016, at which time the Court reserved decision. (Dkt. 139).

MOTION TO DISMISS FOR LACK OF STANDING

The Court first considers the issue of standing. The Excellus Defendants raise two sets of standing arguments. First, the Excellus Defendants argue that those Plaintiffs “who do not allege that they have suffered any misuse of their personally identifiable information”—the “non-misuse” Plaintiffs—have not alleged injury-in-fact. (Excellus Mot. at 5-9). Second, the Excellus Defendants argue that the “misuse” Plaintiffs have not alleged facts establishing that their injuries are fairly traceable to the Excellus cyberattack. (*Id.* at 9-12). BCBSA incorporates the Excellus Defendants’ argument that Plaintiff Nina Mottern (the sole named Plaintiff in the Federal Employee class (CMC at ¶ 23)) has not pleaded injury in fact, and it additionally argues that Mottern’s allegation that she experienced fraudulent charges on her credit card is not fairly traceable to the Excellus cyberattack. (BCBSA Mot. at 17 (quoting CMC at ¶ 23)).

I. Fed. R. Civ. P. 12(b)(1)

“A case is properly dismissed for lack of subject matter jurisdiction under Rule 12(b)(1) when the district court lacks the statutory or constitutional power to adjudicate it.” *Makarova v. United States*, 201 F.3d 110, 113 (2d Cir. 2000). To survive a motion

to dismiss under Rule 12(b)(1), Plaintiffs must establish subject matter jurisdiction. *Id.* “A plaintiff asserting subject matter jurisdiction has the burden of proving by a preponderance of the evidence that it exists.” *Id.* “In resolving a motion to dismiss for lack of subject matter jurisdiction under Rule 12(b)(1), a district court . . . may refer to evidence outside the pleadings.” *Id.*

II. General Principles of Article III Standing

“Article III of the Constitution limits federal courts’ jurisdiction to certain ‘Cases’ and ‘Controversies.’” *Clapper v. Amnesty Int’l USA*, 133 S. Ct. 1138, 1146 (2013). One aspect of this case-or-controversy requirement “is that plaintiffs must establish that they have standing to sue.” *Id.* (quotation omitted). “The party invoking federal jurisdiction bears the burden of establishing standing.” *Id.* at 1148 (quotation omitted).

[T]he irreducible constitutional minimum of standing contains three elements. First, the plaintiff must have suffered an “injury in fact”—an invasion of a legally protected interest which is (a) concrete and particularized . . . and (b) actual or imminent, not conjectural or hypothetical Second, there must be a causal connection between the injury and the conduct complained of—the injury has to be fairly . . . traceable to the challenged action of the defendant, and not . . . the result of the independent action of some third party not before the court Third, it must be likely, as opposed to merely speculative, that the injury will be redressed by a favorable decision.

Lujan v. Defs. of Wildlife, 504 U.S. 555, 560-61 (1992) (internal quotation marks, citations, and brackets omitted).

In a class action, the Court considers the injuries of the named plaintiffs, not unnamed class members. That is, class action plaintiffs “must allege and show that they personally have been injured, not that injury has been suffered by other, unidentified

members of the class to which they belong and which they purport to represent.” *Warth v. Seldin*, 422 U.S. 490, 502 (1975). “[I]f none of the named plaintiffs purporting to represent a class establishes the requisite of a case or controversy with the defendants, none may seek relief on behalf of himself or any other member of the class.” *O’Shea v. Littleton*, 414 U.S. 488, 494 (1974).

III. Injury in Fact

As discussed, the first standing element is injury in fact. An injury in fact is “an invasion of a legally protected interest which is (a) concrete and particularized and (b) actual or imminent, not conjectural or hypothetical.” *Lujan*, 504 U.S. at 560 (citations and internal quotation marks omitted).

The Excellus Defendants argue that Plaintiffs who have not alleged any actual misuse of their data—the so-called “non-misuse” Plaintiffs: Matthew Fero, Dwayne Church, Therese Boomershine, and Brenda Caltagarone—have not alleged an injury in fact.² (Excellus Mot. at 5-9). The Excellus Defendants argue that the following alleged injuries are insufficient for standing: increased risk of identity theft, mitigation efforts, overpayment for insurance, and violation of state statutes. (*Id.*).

² BCBSA joins the Excellus Defendants in these arguments, asserting—without elaboration—that Plaintiff Mottern has not pleaded an injury-in-fact. (BCBSA Mot. at 9). The Court rejects this argument: Plaintiff Mottern has alleged some misuse of her data in that she incurred fraudulent charges on her American Express credit card, among other injuries. (CMC at ¶ 23). Thus, the Excellus Defendants’ injury-in-fact challenges, which are based on four plaintiffs having failed to allege any misuse of their personal information, plainly do not apply to Plaintiff Mottern. Accordingly, the Court denies BCBSA’s motion to dismiss Plaintiff Mottern for failing to allege an injury-in-fact.

Plaintiffs argue that they each have alleged an injury-in-fact sufficient to support Article III standing. (Pl. Excellus Opp. at 4-13). Without differentiating, as the Excellus Defendants do, between those who have suffered misuse and those who have not, Plaintiffs claim that they have standing based on alleged present injuries caused by the breach: they have suffered from fraudulent tax returns; unauthorized access to tax information; identity theft; and fraudulent credit or debit charges. (*Id.* at 7). Some Plaintiffs allege “monetary impacts,” such as spending money to remediate or protect from fraudulent activity and experiencing delays in receipt of federal tax returns; Plaintiffs contend that those monetary impacts constitute injury-in-fact. (*Id.*). And, Plaintiffs argue that spending time to deal with the consequences of the breach—including acts such as freezing or monitoring credit and bank statements, reporting identity theft, and completing police reports—also constitutes injury in fact. (*Id.* at 7-8). All Plaintiffs allege that the breach caused them to suffer anxiety and fear, which, according to them, constitutes injury-in-fact. (*Id.* at 8).

A. CMC’s Allegations Regarding The Non-Misuse Plaintiffs

The CMC alleges that Fero, a citizen of New York, received a letter from Excellus notifying him that his PII and PHI, along with the PII and PHI of his wife and two children, may have been compromised in the data breach. (CMC at ¶ 17). He subsequently enrolled himself and his wife in the two-year credit monitoring service offered through Kroll, although he could not enroll his minor children. (*Id.*). The CMC further alleges that, “[a]s a result of the data breach, the Personal Information of Mr. Fero and his family has been compromised, and he has spent time attempting to ensure that his

family is protected from future acts of identity theft or fraud stemming from this data breach.” (*Id.*).

The CMC alleges that Church, a citizen of California, received a letter from Excellus notifying him that his PII and PHI may have been compromised in the data breach. (*Id.* at ¶ 30). He then enrolled in Kroll’s two-year credit monitoring service and ordered a copy of his most recent credit report. (*Id.*). The CMC alleges that, “[a]s a result of the data breach, Mr. Church’s Personal Information has been compromised, and he has been forced to spend time attempting to protect himself from future incidents of identity theft and fraud.” (*Id.*).

The CMC alleges that Boomershine, a citizen of Indiana, received a letter from Lifetime Healthcare Companies notifying her that her PII and PHI may have been compromised in the data breach. (*Id.* at ¶ 33). She subsequently (1) enrolled in Kroll’s two-year credit monitoring service; (2) implemented credit freezes with the three major reporting bureaus; (3) ordered copies of her most recent credit report; (4) filed a police report with the Roanoke Police Department; (5) filed an identity theft report with the FTC; and (6) purchased additional credit monitoring services through Credit Karma. (*Id.*). The CMC further alleges that her “Personal Information has been compromised, and she has spent significant time attempting to protect herself from identity theft and fraud.” (*Id.*).

The CMC alleges that Caltagarone, a citizen of Pennsylvania, “is unsure how or why her information was compromised in the Excellus data breach, but she believes her employer, Cenclear, obtains services from one of the Defendants.” (*Id.* at ¶ 36). She

received a letter from Lifetime Healthcare Companies notifying her that her PII and PHI may have been compromised in the data breach. (*Id.*). The CMC also alleges that her “Personal Information has been compromised” as a result of the data breach. (*Id.*).

B. Increased Risk of Future Identity Theft

1. Parties’ Arguments

The Excellus Defendants argue that the four non-misuse Plaintiffs’ allegations that they suffer an “imminent and certain impending injury flowing from fraud and identity theft posed by their PII and PHI being placed in the hands of unknown third parties,” (CMC at ¶ 167(e)), is conclusory and not “certainly impending,” as required to meet the standard for risk of future harm to support Article III standing. (Excellus Mot. at 5). The Excellus Defendants argue that the fact that other Plaintiffs have alleged misuse of their personal information does not elevate the non-misuse Plaintiffs’ risk of harm to the level of “certainly impending.” (*Id.* at 6).

Plaintiffs argue that they have standing based on “a real risk of future, certainly impending harm, and/or the substantial risk that harm will occur as a result of this breach,” which is sufficient to support Article III standing. (Pl. Excellus Opp. at 8). Plaintiffs point to decisions by “several courts of appeals [that] have determined the substantial risks of future harm posed by a data breach that compromises PII constitutes injury in fact.” (*Id.* at 9). Plaintiffs further assert that the cases on which Defendants rely in support of their argument that Plaintiffs’ risk of harm is not “certainly impending” are distinguishable. (*Id.* at 11-12).

2. Discussion

In 2013, the Supreme Court considered whether future injury satisfies the injury-in-fact requirement for standing in *Clapper*, a case in which the plaintiffs—consisting of attorneys and human rights, labor, legal, and media organizations—challenged the constitutionality of government surveillance of suspected terrorists under the Foreign Intelligence Surveillance Act. *Clapper*, 133 S. Ct. at 1145-46. The Supreme Court ruled that “[t]hreatened injury must be certainly impending to constitute injury in fact, and allegations of possible future injury are not sufficient.” *Id.* at 1147 (brackets, emphasis, and quotation marks omitted). Applying that rule, the Supreme Court concluded that the plaintiffs’ “theory of future injury [wa]s too speculative to satisfy the well-established requirement that threatened injury must be ‘certainly impending,’” *id.* at 1143; that is, the theory of standing “relie[d] on a highly attenuated chain of possibilities” and was only “speculative whether the Government [would] imminently target communications to which [the plaintiffs were] parties,” *id.* at 1148. Yet the Supreme Court also stated in a footnote that it has not always required “plaintiffs to demonstrate that it is literally certain that the harms they identify will come about.” *Id.* at 1150 n.5. The Supreme Court explained that it has, in some instances, found “standing based on a ‘substantial risk’ that the harm will occur, which may prompt plaintiffs to reasonably incur costs to mitigate or avoid that harm.” *Id.*; see also *Spokeo, Inc. v. Robins*, 136 S. Ct. 1540, 1549 (2016) (citing *Clapper* for the proposition that “the risk of real harm” may “satisfy the requirement of concreteness” for the injury in fact requirement).

Before and after *Clapper*, courts have split over whether increased risk of identity theft is sufficient for standing in a data breach case. The Second Circuit has not yet addressed the issue, although it is poised to do so. See *Whalen v. Michael Stores, Inc.*, 153 F. Supp. 3d 577, 579 n.2 (E.D.N.Y. 2015), *appeal docketed*, 2d Cir. 16-260, 16-352. Other circuit courts to have considered the issue have reached different results: the Sixth, Seventh, and Ninth Circuits have found standing based on increased risk of identity theft, while the Third and Fourth Circuits have found such injury too speculative to warrant standing.

Before *Clapper*, in *Krottner v. Starbucks Corp.*, 628 F.3d 1139 (9th Cir. 2010), the Ninth Circuit found that data breach victims had standing based on increased risk of identity theft. *Id.* at 1143-43. In that case, a laptop containing the names, addresses, and social security numbers of 97,000 Starbucks employees was stolen. *Id.* at 1140. Starbucks notified those employees of the theft and offered credit monitoring services, even though there had been “no indication that the private information ha[d] been misused.” *Id.* at 1140-41. One named plaintiff alleged that someone used his Social Security number to attempt to open a bank account following the theft of the laptop. *Id.* at 1141. The Ninth Circuit, noting that “the possibility of future injury may be sufficient to confer standing on plaintiffs,” held that the increased risk of identity theft was an injury in fact because the plaintiffs had alleged “a credible threat of real and immediate harm stemming from the theft of the laptop.” *Id.* at 1142-43.

In another pre-*Clapper* decision, *Reilly v. Ceridian Corp.*, 664 F.3d 38 (3d Cir. 2011), the Third Circuit reached a different result, holding that plaintiffs’ alleged injuries

from increased risk of identity theft were insufficient for standing. *Id.* at 43. In that case, hackers “potentially gained access” to personal information belonging to 27,000 people that was stored on a computer system of a payroll processing company, but “whether the hacker read, copied, or understood” the personal information was unclear. *Id.* at 40. The Third Circuit reasoned that the plaintiffs—victims of that data breach—would have injuries only “*if* the hacker read, copied, and understood the hacked information, and *if* the hacker attempts to use the information, and *if* he does so successfully.” *Id.* at 43 (emphasis in original). The Third Circuit distinguished *Starbucks Corp.*; it reasoned that the threatened harms were more imminent than in the case before it, where there was “no evidence that the intrusion was intentional or malicious. [The plaintiffs] ha[d] alleged no misuse, and therefore, no injury. Indeed, no identifiable taking occurred; all that is known is that a firewall was penetrated.” *Id.* at 44.

After *Clapper*, the Fourth Circuit concluded that the plaintiffs’ alleged injury of increased risk of identity theft was too speculative to constitute an injury-in-fact. *Beck v. McDonald*, No. 15-1395, No. 15-1715, 2017 WL 477781, at *7 (4th Cir. Feb. 6, 2017). In *Beck*, two cases were consolidated for appeal; one case arose out of the theft of a laptop containing unencrypted personal information, while the other arose out of the theft of four boxes of pathology reports containing personal information. *Id.* at *1-3. The Fourth Circuit concluded that plaintiffs’ allegations of standing based on threatened injury of future identity theft was too speculative to constitute an injury-in-fact, reasoning that the plaintiffs had made no claim either that the data thief intentionally targeted the personal information or that any instances of misuse had occurred as a result of the data

breach. *Id.* at *7-8. The Fourth Circuit also reasoned that, even after discovery, no evidence demonstrated that the plaintiffs' information has been misused or that they have suffered identity theft. *Id.* at *8.

Both before and after *Clapper*, the Seventh Circuit has concluded that risk of identity theft is sufficient for standing. In a pre-*Clapper* case, *Pisciotta v. Old National Bancorp*, 499 F.3d 629 (7th Cir. 2007), the plaintiffs had brought a class action against a bank, alleging that it failed to adequately secure their personal information, and as a result, a hacker stole that information. *Id.* at 631. The Seventh Circuit concluded that "the injury-in-fact requirement can be satisfied by a threat of future harm or by an act which harms the plaintiff only by increasing the risk of future harm that the plaintiff would have otherwise faced, absent the defendant's actions." *Id.* at 634 & n.3.

Post-*Clapper*, the Seventh Circuit found that risk of identity theft is sufficient for standing in two data breach cases. The first was *Remijas v. Neiman Marcus Group, LLC*, 794 F.3d 688 (7th Cir. 2015). That case arose from a data breach in which hackers used malware to collect data associated with 350,000 Neiman Marcus store credit cards. In the months after the data breach, more than 9,200 customers found fraudulent charges on their Neiman Marcus credit cards. *Id.* at 690. The complaint alleged that the hackers had actually stolen and misused the store credit card data; as a result, the Seventh Circuit concluded that "the Neiman Marcus customers should not have to wait until hackers commit identity theft or credit-card fraud in order to give the class standing, because there is an 'objectively reasonable likelihood' that such an injury will occur." *Id.* at 693. The Seventh Circuit explained:

At this stage in the litigation, it is plausible to infer that the plaintiffs have shown a substantial risk of harm from the Neiman Marcus data breach. Why else would hackers break into a store's database and steal consumers' private information? Presumably, the purpose of the hack is, sooner or later, to make fraudulent charges or assume those consumers' identities.

Id. Thus, the Seventh Circuit found injuries sufficient for standing based on future injuries—the increased risk of fraudulent charges and the increased risk of identity theft—as well as the time and money spent resolving fraudulent charges and in protecting against future charges. *Id.* at 691-94.

The second post-*Clapper* case was *Lewert v. P.F. Chang's China Bistro, Inc.*, 819 F.3d 963 (7th Cir. 2016), in which the Seventh Circuit followed *Remijas*. There, the Seventh Circuit found that customers of P.F. Chang's restaurant whose credit and debit card data had been stolen in a data breach had “the same kind of future injuries as the *Remijas* plaintiffs did: the increased risk of fraudulent charges and identity theft they face[d] because their data ha[d] already been stolen.” *Id.* at 967. The Seventh Circuit stated that whether the plaintiffs' data was exposed in the breach—something that P.F. Chang's disputed—was immaterial at the pleading stage. *Id.* at 968.

In *Galaria v. Nationwide Mutual Insurance Co.*, Nos. 15-3386/3387, 2016 WL 4728027 (6th Cir. Sept. 12, 2016), the Sixth Circuit found post-*Clapper* that plaintiffs had standing in a case arising out of the theft of their personal information from the computer network of Nationwide Mutual Insurance Company. *Id.* at *1. The Sixth Circuit held that the plaintiffs' allegations that “the theft of their personal data places them at a continuing, increasing risk of fraud and identity theft” were sufficient for standing at the pleading stage of the litigation. *Id.* at *3. The Sixth Circuit reasoned that

speculation about the possibility of future injury was unnecessary when the data had already been stolen and was in the possession of criminals:

Indeed, Nationwide seems to recognize the severity of the risk, given its offer to provide credit-monitoring and identity-theft protection for a full year. Where a data breach targets personal information, a reasonable inference can be drawn that the hackers will use the victims' data for the fraudulent purposes alleged in [p]laintiffs' complaints.

Id. at *3. The Sixth Circuit distinguished the Third Circuit's decision in *Reilly* on the grounds that, unlike in that case, the plaintiffs had alleged an "identifiable taking," that is, the intentional theft of their data. *Id.* at *4. On that point, the Court stated that at the pleading stage, it was required to "accept as true [p]laintiffs' allegations about the nature of the breach and the data stolen, and construe the complaints in [p]laintiffs' favor." *Id.* at *4 n.3.

Like circuit courts, district courts have also reached different conclusions regarding standing based on increased risk of identity theft. One case, on which the Excellus Defendants rely, is *In re Science Applications International Corp. (SAIC) Backup Tape Data Theft Litigation*, 45 F. Supp. 3d 14 (D.D.C. 2014). That case arose out of the theft of data tapes containing personal information of military members and their families. *Id.* at 20. Most plaintiffs alleged injury based on increased risk of identity theft alone; some of those plaintiffs additionally alleged injury based on the time or money spent monitoring their credit or communicating with banks regarding the theft. *Id.* at 21. The *In re SAIC* court, relying on *Reilly*, concluded that neither the increased risk of identity theft, nor the costs of credit monitoring or other preventative measures, constituted an injury in fact for standing purposes. *Id.* at 25-28.

Like *In re SAIC*, other district courts have found no standing and “dismiss[ed] suits where the plaintiffs, even where they alleged that their personal data had been stolen or accessed, did not allege actual misuse of the data.” *Khan v. Children’s Nat’l Health Sys.*, 188 F. Supp. 3d 524, 531 (D. Md. 2016); see *In re Zappos.com, Inc.*, 108 F. Supp. 3d 949, 958-59 (D. Nev. 2015) (finding no standing where last four digits of customers’ credit card were stolen, but plaintiffs had not alleged any unauthorized purchases or other misuse); *Whalen*, 153 F. Supp. 3d at 583 (finding no standing based on increased risk of future harm where plaintiff alleged that “fraudulent use of cards might not be apparent for years” and did not allege any out of pocket costs resulting from data breach); see also *In re SuperValu, Inc.*, No. 14-MD-2586 ADM/TNL, 2016 WL 81792, at *5 (D. Minn. Jan. 7, 2016) (finding that an allegation of a single unauthorized charge on a credit card in the almost a year and a half following a data breach was not traceable to the breach and did not support an inference that the plaintiffs’ credit card information was at substantial risk of misuse because of the breach), *appeal docketed*, 8th Cir. 16-2528; *Peters v. St. Joseph Servs. Corp.*, 74 F. Supp. 3d 847, 854 (S.D. Tex. 2015) (finding injury based on increased risk of future identity theft too speculative because plaintiff “cannot describe how she will be injured without beginning the explanation with the word ‘if’ (quotation and alterations omitted)).

By contrast, in cases where district courts have found standing, the plaintiffs set forth “allegations indicating that some of the stolen data had already been misused, that there was a clear intent to use the plaintiffs’ personal data for fraudulent purposes, or both.” *Khan*, 188 F. Supp. 3d at 531; see *Welborn v. Internal Revenue Serv.*, No. CV 15-

1352 (RMC), 2016 WL 6495399, at *7 (D.D.C. Nov. 2, 2016) (finding that plaintiffs who alleged that “they ha[d] suffered actual identity theft when someone filed false tax returns (and claimed fraudulent refunds) in their names” sufficiently pleaded injury-in-fact, whereas “allegations that they face[d] an increased risk of future harm [did] not satisfy Article III”), *appeal docketed*, D.C. Cir. 16-5365; *In re Target Corp. Data Sec. Breach Litig.*, 66 F. Supp. 3d 1154, 1157-59 (D. Minn. 2014) (finding standing based on “unlawful charges, restricted or blocked access to bank accounts, inability to pay other bills, and late payment charges or new card fees” suffered by the plaintiffs in case arising out of theft of credit and debit card and personal information belonging to Target customers); *In re Adobe Sys., Inc. Privacy Litig. (Adobe)*, 66 F. Supp. 3d 1197, 1214-16 (N.D. Cal. 2014) (finding standing where hackers deliberately targeted Adobe’s servers to steal the plaintiffs’ credit card information and posted some of the stolen data on websites used by hackers); *In re Sony Gaming Networks & Customer Data Sec. Breach Litig.*, 996 F. Supp. 2d 942, 955-58, 962-63 (S.D. Cal. 2014) (finding “allegations that [the plaintiffs’] Personal Information was collected by Sony and then wrongfully disclosed as a result of the intrusion sufficient to establish Article III standing”).

In *Khan*, 188 F. Supp. 3d at 531, the district court rationalized the different outcomes, finding the differences could be explained not because courts had applied different legal standards, but rather because of variations in the factual circumstances:

In the absence of specific incidents of the use of stolen data for identity fraud purposes, district courts have generally found that the increased risk of identity theft does not confer standing. . . . In fact, the only post-*Clapper* cases cited by [Plaintiff] or uncovered by this [c]ourt in which data breach victims were found to have standing all included allegations indicating that

some of the stolen data had already been misused, that there was a clear intent to use the plaintiffs' personal data for fraudulent purposes, or both.

Id. at 531. Thus, the *Khan* court concluded that, “in the data breach context, plaintiffs have properly alleged an injury in fact arising from increased risk of identity theft if they put forth facts that provide either (1) actual examples of the use of the fruits of the data breach for identity theft, even if involving other victims; or (2) a clear indication that the data breach was for the purpose of using the plaintiffs' personal data to engage in identity fraud.” *Id.* at 532. Based on that framework, the *Khan* court concluded that the plaintiff lacked standing to sue because she had not alleged misuse of her data, and the circumstances of the data breach did not clearly indicate that the hackers' purpose was to use personal data to engage in identity fraud. *Id.*

In this case, the four non-misuse plaintiffs—Fero, Church, Boomershine, and Caltagarone—have alleged increased risk of harm, unaccompanied by any concrete misuse of their stolen personal information. (CMC at ¶¶ 17, 30, 33, 36). While they all allege that their personal information was compromised as a result of the data breach, (*see, e.g., id.* at ¶ 17), none allege any facts indicating that the hackers have misused their personal information since the data breach occurred, or that any other suspicious activity has occurred in the three years since the data breach began. This undercuts their assertion that the asserted harm of future identity theft is “certainly impending.” These plaintiffs' claims of injuries do not meet the definition of injury in fact. Their alleged injuries are neither concrete, nor actual and imminent because the alleged injuries rely on a chain of possibilities about the actions of independent actors: these Plaintiffs may suffer some

actual harm if the hacker has the information in a format that is understandable and accessible, and if the hacker intends to commit crimes by misusing it or transmitting it to someone who does, and if the hacker (or other party) can successfully misuse the information. *See Clapper*, 133 S. Ct. at 1150 (“We decline to abandon our usual reluctance to endorse standing theories that rest on speculation about the decisions of independent actors.”).

And, as the Excellus Defendants point out, Mandiant’s investigation of the data breach “did not identify evidence of the collection, staging, or exfiltration of patient data. Although Mandiant did not find evidence of the collection, staging or exfiltration of patient data, Mandiant was unable to rule out the possibility the attacker accessed patient data based on the available log data.” (Dkt. 123); *see also Makarova*, 201 F.3d at 113 (explaining that, in ruling on a 12(b)(1) motion, a court may consider materials outside the pleadings). Thus, even though Plaintiffs allege that their personal information was actually stolen (CMC at ¶ 167(a)), the fact that Mandiant’s investigation did not reveal collection or exfiltration of that data suggests there is not a clear indication from the circumstances of the data breach that the cyber attackers breached Excellus’s networks in order to use these four Plaintiffs’ personal information to commit identity fraud against them. *See Khan*, 188 F. Supp. 3d at 532. Accordingly, the Court finds the alleged harm of increased risk of identity fraud too speculative to support standing for these four plaintiffs.

C. Alternative Bases for Standing

As an initial matter, the Court notes that Plaintiffs have not responded to the Excellus Defendants' arguments that the four non-misuse plaintiffs lack standing based on their alleged mitigation efforts, overpayment for health insurance, diminution in value of personal information, and violations of state statutes. (*See generally* Pl. Excellus Opp.). Some "courts in this circuit have held that a plaintiff's failure to respond to contentions raised in a motion to dismiss constitutes an abandonment of the applicable claims." *Bond v. City of N.Y.*, No. 14-CV-2431(RRM) (VVP), 2015 WL 5719706, at *8 (E.D.N.Y. Sept. 28, 2015) (citing *McLeod v. Verizon New York*, 995 F. Supp. 2d 134, 143-44 (E.D.N.Y. 2014) (collecting cases)). Even if Plaintiffs had responded to the Excellus Defendants' arguments regarding these bases for standing, as discussed below, the Court finds these alternative bases insufficient.

1. Mitigation Efforts

The Excellus Defendants argue that alleged mitigation efforts by the non-misuse Plaintiffs—that is, Boomershine's purchase of additional credit monitoring services (CMC at ¶ 33), and Boomershine, Fero, and Church having "spent time" to protect themselves (*id.* at ¶¶ 17, 30, 33)—are insufficient to establish standing. (Excellus Mot. at 7). The Court agrees.

In *Clapper*, the Supreme Court held that plaintiffs "cannot manufacture standing merely by inflicting harm on themselves based on their fears of hypothetical future harm that is not certainly impending." 133 S. Ct. at 1151. The Supreme Court thus rejected the argument that the cost of measures taken to protect plaintiffs' confidentiality of

communications against surveillance could confer standing, reasoning that, “[i]f the law were otherwise, an enterprising plaintiff would be able to secure a lower standard for Article III standing simply by making an expenditure based on a nonparanoid fear.” *Id.*

This rule from *Clapper* has been applied in the data breach context, such that courts have concluded that mitigation efforts following a data breach do not confer standing where the alleged harm is not imminent. *See Beck*, 2017 WL 477781, at *10 (“[T]hese self-imposed harms cannot confer standing.”); *Remijas*, 794 F.3d at 694 (concluding, based on *Clapper*, that “[m]itigation expenses do not qualify as actual injuries where the harm is not imminent”); *Reilly*, 664 F.3d at 46 (concluding that “alleged time and money expenditures to monitor . . . financial information do not establish standing, because costs incurred to watch for a speculative chain of future events based on hypothetical future criminal acts are no more ‘actual’ injuries than the alleged ‘increased risk of injury’”); *In re SuperValu, Inc.*, 2016 WL 81792, at *7 (stating that “the cost to mitigate the risk of future harm does not constitute an injury in fact unless the future harm being mitigated against is itself imminent”); *Whalen*, 153 F. Supp. 3d at 581 (rejecting argument that mitigation expenses confer standing).

Having concluded that the increased risk of identity theft is not imminent for these four plaintiffs, the non-misuse plaintiffs’ mitigation efforts against that future harm cannot confer standing.

2. Overpayment Allegations

The Excellus Defendants argue that Plaintiffs cannot establish injury-in-fact based on their alleged overpayment for health insurance. (Excellus Mot. at 7-8). The Court

agrees. “[A] number of courts have rejected an ‘overpayment’ theory of damages as an injury-in-fact for standing purposes.” *In re Cmty. Health Sys., Inc.*, No. 15-CV-222-KOB, 2016 WL 4732630, at *8 (N.D. Ala. Sept. 12, 2016); *see Khan*, 188 F. Supp. 3d at 533 (finding no standing based on overpayment allegations where plaintiff did “not allege any facts showing that she overpaid for . . . services or that she would have sought those services from another provider had she been aware of the hospital’s allegedly lax data security”); *Carlsen v. GameStop, Inc.*, 112 F. Supp. 3d 855, 861 (D. Minn. 2015) (finding no standing based on overpayment theory and stating that “[c]ourts have generally found ‘overpayment’ theories insufficient to establish injury, even in situations involving highly sensitive [personal information]”); *In re Zappos.com, Inc.*, 108 F. Supp. 3d at 962 n.5 (finding no standing based on “diminished value of the services provided by Zappos” because plaintiffs failed to “allege facts showing how the price they paid for [Zappos’s] goods incorporated some particular sum that was understood by both parties to be allocated towards the protection of customer data”); *In re SAIC*, 45 F. Supp. 3d at 30 (rejecting overpayment theory, stating, “[t]o the extent that Plaintiffs claim that some indeterminate part of their premiums went toward paying for security measures, such a claim is too flimsy to support standing.”); *see Lewert*, 819 F.3d at 968 (expressing, *in dicta*, skepticism about plaintiffs’ argument that “the cost of their meals is an injury because they would not have dined at P.F. Chang’s had they known of its poor data security”); *see also Remijas*, 794 F.3d 688, 696 (7th Cir. 2015) (refraining “from deciding whether the overpayment for Neiman Marcus products . . . might suffice as

injuries under Article III” but acknowledging that the court was “dubious” that the overpayment theory alone would have sufficed for standing).

Here, as the Excellus Defendants rightly point out, the CMC lacks any factual allegations that would support the claim that Plaintiffs paid a specific amount of money for data security. (See CMC at ¶ 167(h) (claiming “overpayment for health insurance . . . , in that a portion of the price for insurance or other services paid by Plaintiffs and Class Members to Defendants was for the costs of Defendants to take reasonable and adequate security measures”). Accordingly, Plaintiffs’ alleged overpayment is not a basis for standing.

3. Diminution in Value

The Excellus Defendants argue that Plaintiffs’ allegation that they have suffered a diminution in value of their personal information does not support standing because Plaintiffs have not alleged any facts showing that the breach deprived them of any value. (Excellus Mot. at 8-9). Courts have rejected allegations that the diminution in value of personal information can support standing. See *Welborn*, 2016 WL 6495399, at *8 (“Courts have routinely rejected the proposition that an individual’s personal identifying information has an independent monetary value.”); *Khan*, 188 F. Supp. 3d at 533 (rejecting standing based on diminution in value theory because plaintiff did not “explain how the hackers’ possession of that information has diminished its value, nor does she assert that she would ever actually sell her own personal information”); *Whalen*, 153 F. Supp. 3d at 582 (“[W]ithout allegations about how her cancelled credit card information lost value, [plaintiff] does not have standing on this ground.”); *In re SAIC*, 45 F. Supp. 3d

at 30 (“As to the value of their personal and medical information, Plaintiffs do not contend that they intended to sell this information on the cyber black market in the first place, so it is uncertain how they were injured by this alleged loss. Even if the service members did intend to sell their own data—something no one alleges—it is unclear whether or how the data has been devalued by the breach.”). Although Plaintiffs’ CMC alleges that the information compromised in the Excellus data breach commands a high price on the black market (CMC at ¶ 162), the CMC lacks factual allegations to support the proposition that their personal information was made less valuable to them as a result of the breach, or that the data breach negatively impacted the value of their data such that Plaintiffs could not use or sell it. Thus, because Plaintiffs have not alleged any facts regarding how the data breach has led to a diminution in the value of their personal information, there can be no standing on this basis.

4. Violation of State Statutes

Finally, the Excellus Defendants argue that the asserted violations of various state statutes do not confer standing in federal court. (Excellus Mot. at 9). The Court agrees. *See Spokeo*, 136 S. Ct. at 1549 (“Article III standing requires a concrete injury even in the context of a statutory violation.”); *Hollingsworth v. Perry*, 133 S. Ct. 2652, 2667 (2013) (“[S]tanding in federal court is a question of federal law, not state law. And no matter its reasons, the fact that a State thinks a private party should have standing to seek relief for a generalized grievance cannot override our settled law to the contrary.”); *see also Khan*, 188 F. Supp. 3d at 534 (concluding, in a data breach case, that violations of state statutes and common law cannot establish Article III standing).

D. Conclusion

Based on the foregoing, the Court grants the Excellus Defendants' motion to dismiss the four non-misuse plaintiffs (Fero, Church, Boomershine, and Caltagarone) for lack of standing on the basis that they have not alleged an injury-in-fact. The Court dismisses these plaintiffs' claims without prejudice, as the Court's conclusion would not necessarily bar these plaintiffs from asserting a claim in the event that they suffered an actual misuse. Nonetheless, because there is no information before the Court that these plaintiffs could presently replead their claims to allege actual misuse, the Court declines to grant leave to replead.

IV. Causation

The second element of standing—causation—requires “a causal connection between the injury and the conduct complained of.” *Lujan*, 504 U.S. at 560. The harm alleged must be “fairly . . . trace[able] to the challenged action of the defendant, and not injury that results from the independent action of some third party not before the court.” *Simon v. E. Ky. Welfare Rights Org.*, 426 U.S. 26, 41-42 (1976). While a plaintiff's injury must be “fairly traceable” to a defendant's actions, the causal connection element of standing “does not create an onerous standard. For example, it is a standard lower than that of proximate causation. . . . A defendant's conduct that injures a plaintiff but does so only indirectly, after intervening conduct by another person, may suffice for Article III standing.” *Carter v. HealthPort Techs., LLC*, 822 F.3d 47, 55-56 (2d Cir. 2016) (citations omitted).

A. The Parties' Arguments

The Excellus Defendants argue that the “misuse” Plaintiffs “have not pleaded any facts to tie their particular allegations of misuse to the Excellus cyberattack as opposed to any other possible source.” (Excellus Mot. at 10). The Excellus Defendants also argue that the alleged forms of misuse—phishing emails, fraudulent charges on credit or debit cards, tax fraud, and identity theft—are fairly common and could have been the result of the actions of some third party not before the Court or another data breach of recent years. (*Id.*). To that end, the Excellus Defendants, citing *In re SAIC*, 45 F. Supp. 3d at 27, report the statistic that identity theft affects 3.3% of the population. (*Id.*). The Excellus Defendants also argue that the alleged harms of phishing emails and fraudulent charges are not traceable when Plaintiffs have not alleged that they provided email addresses or payment card information to Excellus. (*Id.* at 10-11).

Plaintiffs respond to the Excellus Defendants’ argument stating, “[t]raceability does not require plaintiffs to rule out every possible alternative cause at the pleading stage,” and that several courts have rejected similar arguments that an injury cannot be fairly traceable if it is a common injury. (Pl. Excellus Opp. at 25-26). According to Plaintiffs, in the data breach context, “no court” has accepted a traceability argument like the one advanced by the Excellus Defendants. (*Id.* at 25-26).

BCBSA argues that Mottern’s injuries cannot be deemed fairly traceable when she has not alleged that she provided her credit card information to Excellus, or that she paid her premiums to any Defendants directly or by credit card. (BCBSA Mot. at 9). BCBSA also argues that Mottern “alleges no facts demonstrating that the fraudulent charges, or

even the cyberattack itself, are fairly traceable to any conduct by BCBSA.” (*Id.*). BCBSA identifies three purported deficiencies in that regard: First, according to BCBSA, Mottern has engaged in impermissible group pleading by lumping BCBSA in with either Excellus or with all Defendants. (*Id.* at 10). Second, BCBSA argues that Mottern’s allegations are conclusory, as she asserts “‘failings’ by Defendants without identifying what limitations, ‘best practices,’ or ‘safeguards’ BCBSA should have employed, and point[s] to no actual *misconduct* by BCBSA that resulted in injury to Plaintiffs.” (*Id.*). Third, BCBSA argues that “conclusory statements that BCBSA violated a statute, without more, are insufficient to confer Article III standing.” (*Id.*).

Plaintiffs respond to BCBSA by arguing that Mottern’s injuries are fairly traceable: the requirement is not onerous and may be satisfied even when the injury is indirectly traceable due to the intervening conduct by another person. (Pl. BCBSA Opp. at 4). Plaintiffs maintain that their allegations concerning BCBSA are sufficient: according to the CMC, BCBSA contracted to ensure that federal employees, like Mottern, benefitted from reasonable data security, that BCBSA, as agent for Excellus, failed to provide that security in certain respects, and that the failures led to identity theft, fraud, and the imminent risk of future harm. (*Id.* at 4-5 (citing CMC at ¶¶ 82-95, 134, 142-45)).

B. “Fairly Traceable” in Data Breach Context

In the data breach context, courts have rejected the argument that plaintiffs’ injuries are not fairly traceable when their information could have been compromised during a different data breach in recent years. *See Remijas*, 794 F.3d at 696. In *Remijas*,

for example, the Seventh Circuit concluded that “[t]he fact that Target or some other store [besides Neiman Marcus] might have caused the plaintiffs’ private information to be exposed does nothing to negate the plaintiffs’ standing to sue.” *Id.* At the pleading stage, the Seventh Circuit found it sufficient that Neiman Marcus admitted that customers’ credit cards had been exposed and that the retailer had notified them that their personal information was at risk. *Id.* The Seventh Circuit explained that Neiman Marcus’ argument was better raised as a defense in a later stage in the litigation: “If there are multiple companies that could have exposed the plaintiffs’ private information to the hackers, then ‘the common law of torts has long shifted the burden of proof to defendants to prove that their negligent actions were not the ‘but-for’ cause of the plaintiff’s injury.’” *Id.* (citations and quotations omitted).

Other courts have similarly rejected challenges to standing based on traceability in the data breach context, finding the challenge better suited for a later stage of the litigation. *See Lewert*, 819 F.3d at 969 (rejecting the argument that fraudulent charges could not be attributed to data breach at P.F. Chang’s, and explaining that the argument that there are potential alternative causes for plaintiffs’ injuries may be pursued at merits phase); *In re Zappos.com, Inc.*, 2016 WL 2637810, at *6 (rejecting traceability argument because “[w]hether or not . . . [p]laintiffs’ allegations suffer from defects that prevent them from ultimately prevailing in the case, the allegations show the connection between the alleged injury and breach is more than just hypothetical or tenuous”); *In re Target Corp.*, 66 F. Supp. 3d at 1159 (“Plaintiffs’ allegations plausibly allege that they suffered injuries that are ‘fairly traceable’ to Target’s conduct. . . . This is sufficient at this stage

to plead standing. Should discovery fail to bear out Plaintiffs' allegations, Target may move for summary judgment on the issue.").

On the other hand, in *In re SAIC*, 45 F. Supp. 3d at 31-33, the court concluded that some of the plaintiffs did not meet the causation requirement because, while they had alleged unauthorized charges on their credit and debit cards or that money was withdrawn from their bank accounts, none had alleged that credit card, debit card, or bank account information was on the stolen tapes. The district court in *In re: Community Health Systems, Inc.* similarly found that the "fairly traceable" element exists for purposes of Article III case or controversy standing "when at least one instance of misuse was pled that would have a logical connection to the data stolen." 2016 WL 4732630 at *12. Thus, as in *In re SAIC*, the *In re: Community Health Systems, Inc.* court dismissed, for example, plaintiffs who alleged unauthorized credit card charges but who did not allege that the data breach included credit card information. *See id.* Similarly relying on *In re SAIC*, the D.C. district court in *Welborn* found that a plaintiff who had alleged a potential compromise of her personal information, followed by an instance of fraudulent activity in her financial accounts, such as the removal of funds, could not meet the traceability requirement because "[i]t [wa]s not clear that the type of data obtained from the theft . . . was necessarily used in the removal of funds." 2016 WL 6495399, at *9. That plaintiff thus failed to "put forward facts showing that [her] injuries [could] be traced to the specific data incident of which [she] complain[ed] and not to any previous theft or data loss incident." *Id.*

C. Application

The Court finds Defendants' arguments unpersuasive. The CMC plausibly alleges that the various forms of misuse are "fairly traceable" to the data breach on the Excellus networks. At this early stage of the litigation, Plaintiffs' allegations are sufficient. They have alleged that the Defendants failed to safeguard their personal information—including names, dates of birth, social security numbers, member identification numbers, home addresses, telephone numbers, and financial information (CMC at ¶ 56)—and, as a direct result, hackers gained access to their personal information. They have also alleged that BCBSA contracted to ensure that federal employees, like Mottern, benefitted from reasonable data security, that BCBSA, as agent for Excellus, failed to provide that security in certain respects, and that the failures led to identity theft, fraud, and the imminent risk of future harm. (*Id.* at ¶¶ 82-95, 134, 142-45). These alleged chains of events are plausible, and, given that the causation element of standing is not an onerous hurdle, the Court finds that the Plaintiffs have sufficiently alleged this requirement and need not rule out alternative sources of their injuries. Thus, Defendants' motion to dismiss the remaining Plaintiffs' claims for lack of the causation aspect of standing is denied.

MOTIONS TO DISMISS FOR FAILURE TO STATE A CLAIM

Defendants further argue that, even if Plaintiffs did have standing, they have failed to state a claim.

I. Rule 12(b)(6) Standard

“To survive a motion to dismiss, a complaint must contain sufficient factual matter, accepted as true, to ‘state a claim to relief that is plausible on its face.’” *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (quoting *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007)). “A claim has facial plausibility when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged. The plausibility standard is not akin to a ‘probability requirement,’ but it asks for more than a sheer possibility that a defendant has acted unlawfully.” *Id.* (internal citations omitted). Generally, the Court must accept as true all of the allegations contained in the complaint. *See id.* That rule does not apply to legal conclusions, however: “[t]hreadbare recitals of the elements of a cause of action, supported by mere conclusory statements . . . are not entitled to the assumption of truth.” *Id.*; *see also Twombly*, 550 U.S. at 555 (stating that the Court is “not bound to accept as true a legal conclusion couched as a factual allegation”).

The plausibility standard “asks for more than a sheer possibility” that a defendant has acted unlawfully. *Iqbal*, 556 U.S. at 678. “Where a complaint pleads facts that are ‘merely consistent with’ a defendant’s liability, it ‘stops short of the line between possibility and plausibility of ‘entitlement to relief.’” *Id.* (quoting *Twombly*, 550 U.S. at 557). “Determining whether a complaint states a plausible claim for relief [is] . . . a

context-specific task that requires the reviewing court to draw on its judicial experience and common sense.” *Id.* at 679. Plausibility is “a standard lower than probability.” *Anderson News, L.L.C. v. Am. Media, Inc.*, 680 F.3d 162, 184 (2d Cir. 2012). “[A] given set of actions may well be subject to diverging interpretations, each of which is plausible,” and “[t]he choice between or among plausible inferences or scenarios is one for the factfinder.” *Id.* A court “may not properly dismiss a complaint that states a plausible version of the events merely because the court finds that a different version is more plausible.” *Id.* at 185.

II. Contract-Based Claims

Defendants seek dismissal of Plaintiffs’ contract-based claims: (1) breach of express contract; (2) breach of the implied covenant of good faith and fair dealing; and (3) third party beneficiary claim for breach of contract under federal law.

A. Breach of Express Contract Claim (Third Claim for Relief)

Plaintiffs’ third claim for relief alleges breach of contract against the Excellus Defendants for breaching an express promise to ensure data security. (CMC at ¶¶ 208-22). According to Plaintiffs, three types of contracts are at issue in this case. (*Id.* at ¶ 209). First, some Plaintiffs “purchased individual insurance plans from Excellus and/or the Affiliate Defendants.” (*Id.*). Second, some Plaintiffs “enrolled pursuant to the terms of a group contract with Excellus and/or the Affiliate Defendants.” (*Id.*). Third, some plaintiffs “entered contracts with Defendants as healthcare providers.” (*Id.*). All contracts were “entered into prior to the disclosure of the Excellus data breach.” (*Id.* at ¶ 213). Further, all contracts “incorporated, either by express provision or attachment, or

incorporation by reference,” the relevant Defendants’ privacy policies pertaining to personal information. (*Id.* at ¶¶ 81, 215-17). According to Plaintiffs, Excellus breached those privacy policies by “violating the commitment to maintain the confidentiality and security of Personal Information compiled by Defendants and stored in the Excellus Networks,” and by “failing to comply with their policies and applicable laws, regulations, industry standards, and best practices for data security and protecting the confidentiality of Personal Information.” (*Id.* at ¶ 218).

The Excellus Defendants argue that this claim should be dismissed because, even if one assumes that the privacy policy is incorporated into an express contract between Defendants and each plaintiff, those privacy notices do not contain a definite material term promising Plaintiffs a particular level of data security. (Excellus Mot. at 13-14). According to the Excellus Defendants, those privacy notices merely contain disclosures concerning how Excellus may use healthcare information. (*Id.* at 13). The Excellus Defendants argue that Plaintiffs have not alleged any breach of the privacy notices’ two basic statements regarding data security: (1) that Excellus has a security coordinator to detect and prevent data breaches; and (2) that all computer systems that contain personal information have security protections. (*Id.* at 13-14).

In opposition, Plaintiffs argue that the privacy notices identified in the CMC (CMC at ¶¶ 60-81), contain the following definite promises:

- “We are committed to safeguarding your protected health information (PHI).” (*Id.* ¶ 61 & Ex. A; *see also id.* ¶ 69 & Exs. B–H.)

- Defendants “will not give out your nonpublic personal information to anyone unless we are permitted to do so by law.” (*Id.* ¶ 62 & Ex. A; *see also id.* ¶ 69 & Exs. B–H.)
- “It is our policy to keep all information about you confidential in all settings.” (*Id.* at Ex. A; *see also id.* at Exs. B, E–H.)
- “[W]e have a security coordinator to detect and prevent security breaches.” (*Id.* ¶ 64 & Ex. A; *see also id.* at Exs. B, E–H.)
- “[A]ll computer systems that contain personal information have security protections.” (*Id.* ¶ 64 & Ex. A; *see also id.* at Exs. B, E–H.)
- “We will notify you should there be a breach of unsecured information.” (*Id.* ¶ 65 & Ex. A; *see also id.* at Exs. B, E–H.)

(Pl. Excellus Opp. at 14–15). According to Plaintiffs, these statements are “simple, unambiguous, explicit promises of data security,” and Defendants breached them by allowing hackers long-term access to Plaintiffs’ personal information. (*Id.* at 16).

Under New York law,³ a breach of contract claim has four elements: “(1) a contract; (2) performance of the contract by one party; (3) breach by the other party; and (4) damages.” *First Inv’rs Corp. v. Liberty Mut. Ins. Co.*, 152 F.3d 162, 168 (2d Cir. 1998). Here, the parties dispute whether Plaintiffs allege facts sufficient to show the first of those elements: an enforceable contract.

It is a “well-settled principle of New York law that ‘[i]f an agreement is not reasonably certain in its material terms, there can be no legally enforceable contract,’ which principle ensures that ‘courts will not impose contractual obligations when the parties did not intend to conclude a binding agreement.’” *Hudson & Broad, Inc. v. J.C.*

³ Both the Excellus Defendants and Plaintiffs make their arguments under New York law. (*See* Excellus Mot. at 13–14; Pl. Excellus Opp. at 15–16).

Penney Corp., 553 F. App'x 37, 39 (2d Cir. 2014) (quoting *Cobble Hill Nursing Home v. Henry & Warren Corp.*, 74 N.Y.2d 475, 482 (1989)); *see also Cauff, Lippman & Co. v. Apogee Fin. Grp., Inc.*, 807 F. Supp. 1007, 1020 (S.D.N.Y. 1992) (“An enforceable contract must contain sufficiently explicit terms to enable a court to determine the intent of the parties to a reasonable degree of certainty, . . . and it must be definite enough to be susceptible to judicial interpretation.”). However, “New York has not applied the definiteness doctrine rigidly, recognizing that parties are often imprecise in their use of language. Striking down a contract as indefinite and in essence meaningless is at best a last resort.” *Shaw v. Shaw*, 356 F. Supp. 2d 383, 386 (S.D.N.Y. 2005) (quotations omitted); *see also Cobble Hill Nursing Home, Inc.*, 74 N.Y.2d at 483 (“[A]t some point virtually every agreement can be said to have a degree of indefiniteness, and if the doctrine is applied with a heavy hand it may defeat the reasonable expectations of the parties in entering into the contract.”).

Based on the foregoing, the Court finds the Excellus Defendants’ argument unpersuasive. Assuming, as the parties do and as it is alleged in the CMC (CMC at ¶¶ 216-17), that the privacy notices are incorporated by reference in the contracts between the parties, the statements from the privacy policies identified by Plaintiffs plausibly could be read to reflect a definite promise by Excellus to maintain the security of the personal information that it collected and stored on its networks. (*Id.* at ¶ 218). Because Plaintiffs have stated a breach of contract claim that is plausible on its face, the Court denies the Excellus Defendants’ motion to dismiss this claim for relief.

B. Breach of Implied Covenant of Good Faith and Fair Dealing (Fourth Claim for Relief)

Plaintiffs also allege a breach of the implied covenant of good faith and fair dealing against the Excellus Defendants. (*Id.* at ¶¶ 223-32). Plaintiffs allege that their contracts with the Excellus Defendants were subject to an implied covenant that the Excellus Defendants “would act fairly, reasonably, and in good faith in carrying out their contractual obligations to protect the confidentiality of Plaintiffs’ and Class Members’ Personal Information and to comply with industry standards and best practices, as well as federal and state law and applicable regulations for the security of this information.” (*Id.* at ¶ 225). Plaintiffs allege that, even if Defendants did not breach an express promise in the contracts as alleged in the third claim for relief, Excellus Defendants’ breaches of the covenant of good faith and fair dealing included:

failing to implement reasonable and adequate security measures consistent with industry standards and best practices to protect and limit access to the Personal Information contained in the Excellus Networks; permitting unrestricted access to the Personal Information in the database; and failing to implement reasonable auditing procedures to detect and halt the unauthorized extraction of Personal Information from the database.

(*Id.* at ¶ 227).

The Excellus Defendants contend that this claim should be dismissed, arguing that Plaintiffs cannot invoke an implied covenant of good faith and fair dealing to protect an additional benefit for which the parties did not bargain; that is, Plaintiffs cannot invoke an implied covenant to add to the contract a substantive provision—a promise regarding data security—that was not contemplated by and included by the parties. (Excellus Mot. at 14-15). The Excellus Defendants also argue that Plaintiffs cannot simultaneously

plead breach of contract and implied covenants claims under New York law when the factual predicate for each claim is the same. (Dkt. 133 (“Excellus Reply”) at 12).

Plaintiffs argue that they do not seek to add substantive provisions to the contracts; rather, they allege that Defendants “fail[ed] to conform to applicable data security industry standards and best practices. This failure deprived Plaintiffs of the benefits of their agreements with Defendants—namely, confidentiality of their PHI and PII.” (Pl. Excellus Opp. at 17). In other words, according to Plaintiffs, Defendants’ failure to comply with those standards and best practices, although not expressly forbidden by any contractual provision, deprived Plaintiffs of the right to benefits under their contractual agreement with Defendants. (*See id.*).

“Under New York law, a covenant of good faith and fair dealing is implied in all contracts.” *Fishoff v. Coty Inc.*, 634 F.3d 647, 653 (2d Cir. 2011). This implied covenant “embraces a pledge that neither party shall do anything which will have the effect of destroying or injuring the right of the other party to receive the fruits of the contract.” *Id.* (quoting *511 West 232nd Owners Corp. v. Jennifer Realty Co.*, 98 N.Y.2d 144, 153 (2002) (citations and internal quotation marks omitted). In other words, the covenant of good faith and fair dealing “is breached when a party acts in a manner that, although not expressly forbidden by any contractual provision, would deprive the other party of the right to receive the benefits under the agreement.” *Williamson Acquisition, Inc. v. PNC Equity Mgmt. Corp.*, Nos. 03-CV-6666T, 04-CV-6259T, 2010 WL 276199, at *7 (W.D.N.Y. Jan. 15, 2010) (quoting *Skillgames LLC v. Brody*, 1 A.D.3d 247 (1st Dep’t

2003), *aff'd sub nom. Argilus, LLC v. PNC Fin. Servs. Grp., Inc.*, 419 F. App'x 115 (2d Cir. 2011).

Breach of the implied duty of good faith and fair dealing “is merely a breach of the underlying contract.” *Nat'l Mkt. Share, Inc. v. Sterling Nat'l Bank*, 392 F.3d 520, 525 (2d Cir. 2004); *see also Fishoff*, 634 F.3d at 653 (“A breach of the duty of good faith and fair dealing is considered a breach of contract.”). Therefore, “raising both claims in a single complaint is redundant, and courts confronted with such complaints under New York law regularly dismiss any freestanding claim for breach of the covenant of fair dealing.” *Jordan v. Verizon Corp.*, No. 08 Civ. 6414 (GEL), 2008 WL 5209989, at *7 (S.D.N.Y. Dec. 10, 2008) (citing *Canstar v. J.A. Jones Const. Co.*, 212 A.D.2d 452 (1st Dep't 1995)); *accord Netologic, Inc. v. Goldman Sachs Grp., Inc.*, 110 A.D.3d 433, 434 (1st Dep't 2013) (dismissing implied covenant claim as duplicative of breach of contract claims “since both claims arise from the same facts and seek identical damages for each alleged breach” (internal quotation marks and citation omitted)). “Consequently, a claim for breach of the implied covenant of good faith can survive a motion to dismiss only if it is based on allegations different from those underlying the accompanying breach of contract claim.” *JPMorgan Chase Bank, N.A. v. IDW Grp., LLC*, No. 08 Civ. 9116(PGG), 2009 WL 321222, at *5 (S.D.N.Y. Feb. 9, 2009) (internal quotation marks omitted).

The Court finds that Plaintiffs' implied covenant claim must be dismissed as duplicative of their breach of contract claim because both claims arise from the same facts and seek the same damages for each alleged breach. That is, both the breach of

contract claim and implied covenant claim arise out of the Excellus Defendants' failure to protect the confidentiality of Plaintiffs' personal information and to comply with policies, industry standards, and best practices for data security. (*Compare* CMC at ¶ 218 (alleging breach of express contract by "violating the commitment to maintain the confidentiality and security of Personal Information" and by "failing to comply with their policies and applicable laws, regulations, industry standards, and best practices for data security and protecting the confidentiality of Personal Information"), *with id.* at ¶ 227 (alleging breach of implied covenant by "failing to implement reasonable and adequate security measures consistent with industry standards and best practices to protect and limit access to the Personal Information contained in the Excellus Networks; permitting unrestricted access to the Personal Information in the database; and failing to implement reasonable auditing procedures to detect and halt the unauthorized extraction of Personal Information from the database")). Accordingly, the Court grants the Excellus Defendants' motion to dismiss Plaintiffs' claim for breach of the implied covenant of good faith and fair dealing, although the dismissal is without prejudice. Plaintiffs may not replead this claim as a separate cause of action because it would be futile. *See Jordan*, 2008 WL 5209989, at *7 (denying leave to replead duplicative claim for breach of an implied covenant of good faith and fair dealing on the ground that it would be futile). However, Plaintiffs may pursue any alleged breach of the implied covenant of good faith and fair dealing as part of their underlying breach of contract claim.

C. Third-Party Beneficiary Claim for Breach of Contract Under Federal Law (Fifth Claim for Relief)

Plaintiffs also assert a third party beneficiary claim for breach of contract under federal law against Excellus and BCBSA, based on the following allegations. (*Id.* at ¶¶ 233-46). “BCBSA, acting as agent for, and on behalf of, Excellus, entered into a valid, binding, and enforceable express contract with OPM to provide insurance and other benefits under the Federal BCBS Plan.” (*Id.* at ¶ 234). Under this contract (known as Contract No. CS 1039), BCBSA:

promised, among other things: . . . to take reasonable measures to protect the security and confidentiality of Federal Plaintiffs’ . . . Personal Information, including through the measures described in the Notice of Privacy Practices for the BCBS Plan; and . . . to protect Federal Plaintiffs’ . . . Personal Information in compliance with federal and state laws, regulations, and industry standards.

(*Id.* at ¶ 235). Those “Federal Plaintiffs”—who are current and former federal employees and annuitants who obtained coverage under the Federal BCBS Plan, including Mottern—allege that they “are intended third-party beneficiaries of the data security provisions in the contract between BCBSA . . . and OPM, and are entitled to directly enforce its terms.” (*Id.* at ¶ 242; *see also id.* at ¶ 87). Included in the Federal BCBS Contract are data security provisions that are intended to benefit Plaintiffs. (*Id.* at ¶ 243). They allege that “BCBSA . . . agreed to protect the PII of the Federal BCBS Plan Enrollees,” (*id.* at ¶ 89), and further “agreed to specific obligations with respect to protecting this and other sensitive personal information,” (*id.* at ¶ 90).

1. Background

The Federal Employee Health Benefits Act of 1959 (“FEHBA”), 5 U.S.C. §§ 8901 *et seq.*, “establishes a comprehensive program of health insurance for federal employees” and “authorizes the Office of Personnel Management (OPM) to contract with private carriers to offer federal employees an array of health-care plans.” *Empire Healthchoice Assur., Inc. v. McVeigh*, 547 U.S. 677, 682 (2006); *see also* 5 U.S.C. § 8902(a) (describing OPM’s contracting authority); (CMC at ¶ 83).

One such plan is the BCBS Government-Wide Service Benefit Plan, also known as the Federal Employee Program (“Federal BCBS Plan”). (CMC at ¶ 82). The Plan is governed by Contract No. CS-1039 and its amendments (“Federal BCBS Contract”),⁴ which is entered into pursuant to FEHBA by OPM and BCBSA, acting on behalf of and as agent for local BCBS licensees (like Excellus) that underwrite the Federal BCBS Plan and administer it in their respective localities. (*Id.* at ¶ 84). Plaintiff Mottern is a federal employee or annuitant “who obtained coverage under the BCBS Plan.” (*Id.* at ¶ 86).

⁴ Plaintiffs refer to Contract No. CS 1039 in their CMC, and BCBSA has attached the following documents to their motion to dismiss: (1) a copy of that contract; (2) the 2014 and 2015 amendments to the contract; and (3) the contract’s 2013, 2014, and 2015 Statements of Benefits for the Service Benefit Plan. (Dkt. 111-1; Dkt. 111-2 (Contract No. CS 1039); Dkt. 111-4; Dkt. 111-5 (2014 & 2015 Amendments); Dkt. 111-6; Dkt. 111-7; Dkt. 111-8; Dkt. 111-9 (2013-2015 Statements of Benefits)). Plaintiffs do not dispute that these documents are true and accurate copies of Plaintiffs’ contract with BCBSA and the accompanying statement of benefits; in fact, they also cite to BCBSA’s attachments throughout their opposition. *See, e.g.*, Reply at 8. Therefore, the Court may consider these extra-pleading documents in resolving the motion to dismiss because they are both integral to and referenced in the CMC. *See Goel v. Bunge, Ltd.*, 820 F.3d 554, 558-59 (2d Cir. 2016) (explaining circumstances in which extra-pleading materials may be considered on a motion to dismiss, such as when a document is “incorporated in the complaint by reference” or “integral to the complaint”).

FEHBA requires that the contracts between OPM and the carriers include a “detailed statement of benefits offered and shall include such maximums, limitations, exclusions, and other definitions of benefits as [OPM] considers necessary or desirable.” 5 U.S.C. § 8902(d). Accordingly, the Federal BCBS Contract provides that “[t]he carrier [BCBSA] shall provide the benefits as described in the agreed upon” Statement of Benefits, which is attached to and incorporated into the contract. *See* Federal BCBS Contract at § 2.2(a); (Dkts. 111-6 through 111-9 (2013-2015 Statements of Benefits)). The terms of the contract are renegotiated every year.

Federal regulations provide that enrollees may seek administrative review of disputed “health benefits” claims. Part of that process involves review by OPM and proceeds as follows. First, “[a]ll *health benefits claims* [under the Federal BCBSA contract] must be submitted initially to the carrier of the covered individual’s health benefits plan.” 5 C.F.R. § 890.105(a)(1) (emphasis added). “If the carrier denies a [health benefits] claim (or a portion of a claim), the covered individual may ask the carrier to reconsider its denial.” *Id.* “If the carrier affirms its denial or fails to respond . . . , *the covered individual may ask OPM to review the claim.*” *Id.* (emphasis added). Exhaustion of this review process is required before seeking judicial intervention: “A covered individual must exhaust both the carrier and OPM review processes specified in this section before seeking judicial review of [a] denied claim.” *Id.* Under 5 C.F.R. § 890.107(c), enrollees seeking judicial review of OPM’s resolution of a dispute regarding a health benefits claim must sue OPM, but not the carrier:

A covered individual may seek judicial review of OPM's final action on the denial of a health benefits claim. A legal action to review final action by OPM involving such denial of health benefits *must be brought against OPM and not against the carrier* or carrier's subcontractors. The recovery in such a suit shall be limited to a court order directing OPM to require the carrier to pay the amount of benefits in dispute.

5 C.F.R. § 890.107 (emphasis added).

In addition to reviewing disputed health benefits claims as described above, OPM has the power to manage the contract and the carriers' performance under it. OPM "may prescribe reasonable minimum standards for health benefits plans . . . and for carriers offering the plans," 5 U.S.C. § 8902(e), and "may prescribe regulations necessary to carry out" FEHBA, *id.* § 8913(a). *See also* 48 C.F.R. Chapter 16. OPM "has the right to inspect or evaluate the work performed or being performed under the contract and the premises where the work is being performed," Federal BCBSA Contract § 1.11(a), in addition to the right to audit the carrier, *id.* § 1.11(b). And, OPM has the authority to negotiate the premium rates paid under FEHBA plans. *See* 5 U.S.C. § 8902(i) ("Rates under health benefits plans . . . shall be determined on a basis which, in the judgment of [OPM], is consistent with the lowest schedule of basic rates generally charged for new group health benefit plans issued to large employers.").

OPM also has the authority to take remedial action against a carrier. OPM may penalize a carrier for failing to inform OPM within 10 days of any "Significant Event," that is, an occurrence "that might reasonably be expected to have a material effect upon the [c]arrier's ability to meet its obligations under this contract, including, but not limited to, any of the following" thirteen listed occurrences, none of which explicitly concern

data security.⁵ 48 C.F.R. § 1652.222-70(a). When OPM learns of a Significant Event, OPM “may institute action, in proportion to the seriousness of the event, to protect the interest of Members, including, but not limited to . . . [d]irecting the [c]arrier to take corrective action.” *Id.* § 1652.222-70(b); *see also* Federal BCBSA Contract at § 1.10 (setting forth identical Significant Events clause).

In addition to the “Significant Events” clause, the Federal Contract includes a provision entitled “Correction of Deficiencies,” which provides that “[t]he Carrier shall maintain sufficient financial resources, facilities, providers, staff and other necessary resources to meet its obligations under this contract,” and if OPM determines that the carrier has not met its obligations, it must notify the carrier of the asserted deficiencies. Federal BCBSA Contract at § 1.12(a). The carrier must then present a plan to correct the deficiencies, and pending submission or implementation of those plans, OPM may take “action as it deems necessary to protect the interests of Members,” that is, enrollees such as Mottern. *Id.*

⁵ In its reply, BCBSA has attached a Federal Employees Health Benefits (“FEHB”) Program Carrier Letter from OPM, dated June 22, 2007, stating that “[a]ny breach of security in . . . [FEHB] enrollee data is considered a significant event as defined in Section 1.10 Notice of Significant Events (FEHBA 1652.222-70) of the FEHB Standard Contracts.” (Dkt. 138 at 5). These carrier letters, BCBSA argues, “conclusively demonstrate that the [court in *In re Anthem, Inc. Data Breach Litigation*, 162 F. Supp. 3d 953 (N.D. Cal. 2016) (“*Anthem I*”)] and Plaintiffs are wrong and a data breach *is* a ‘Significant Event over which OPM has exclusive police powers.’” (Dkt. 134 at 9 (quoting Pl. Reply at 14)). The Court declines to consider arguments or evidence raised for the first time in a reply brief. *See ABN Amro Verzekeringen BV v. Geologistics Americas, Inc.*, 485 F.3d 85, 97 n.12 (2d Cir. 2007) (“We decline to consider an argument raised for the first time in a reply brief.”).

The Federal BCBS Contract includes provisions regarding data security. Section 1.30(a) provides that BCBSA is “required . . . to, at a minimum, comply with equivalent privacy and security policies as are required of a ‘covered entity’ under the HIPAA Privacy and Security regulations.” *Id.* § 1.30(a). Section 1.30(d), which was added to the contract in 2014, states that OPM “may recommend that [BCBSA] adopt” certain data security “best practice[s]” that BCBSA must agree to adopt, explain why it is already in compliance, or explain why an alternative best practice is “equally, if not more, appropriate . . . than the [recommended] best practice.” *Id.* § 1.30(d). Section 1.6(b) states that BCBSA “shall . . . hold all medical records, and information relating thereto, of Federal subscribers confidential.” *Id.* § 1.6(b). Moreover, the Statement of Benefits provides that “[w]e will keep your medical and claims information confidential.” (Dkt. 111-7 (2014 Statement of Benefits) at 15).

2. Parties’ Arguments

BCBSA moves to dismiss the third party beneficiary claim, arguing that Mottern is not an intended third-party beneficiary and that enrollees do not have independent rights to enforce that contract against carriers. BCBSA contends that Mottern has not identified any contractual provision stating that the parties intended for the contract to create enforceable rights for enrollees. (BCBSA Mot. at 14). BCBSA argues that only OPM has enforcement authority, as evidenced by the following: (1) the administrative review process for health benefits disputes, which culminates in review by OPM and judicial review of OPM’s decision and which does not allow suit against the carrier; (2) OPM’s broad range of power to remedy poor carrier performance, including, but not

limited to, its power under the Significant Events Clause; (3) OPM's audit rights regarding carrier performance, including a carrier's data security; and (4) FEHBA's objective to ensure uniform administration of FEHBA benefits. (*Id.* at 14-17). The Excellus Defendants adopt and incorporate by reference BCBSA's arguments on this point. (Excellus Mot. at 24-25).

Plaintiffs argue that Mottern is an intended third-party beneficiary of the contract and has the right to enforce it. (Pl. BCBSA Reply at 6). They argue that the parties' clear intent to benefit the members of the Federal Employee class is evident in several ways. First, the contract's language and purpose clearly reflect intent to provide benefits, including data security, to enrollees. (*Id.* at 8-9). Second, such intent is evident because the contract provides that certain rights and benefits, including "health benefits," are enforceable by enrollees through an administrative procedure, which must be exhausted before an enrollee may file a lawsuit against OPM. According to Plaintiffs, "[i]f the contract gave enrollees no enforceable rights (as BCBSA suggests), the contract would not expressly acknowledge the right to challenge health benefits determinations via administrative procedures and, once administrative remedies are exhausted, the courts." (*Id.* at 9-10). Moreover, that administrative procedure applies only where the dispute concerns health benefits; because this dispute regarding data security is not a health benefit dispute, and because data security is promised under the contract, then federal employees must be able to enforce the contract through a breach of contract claim as they do in this case. (*Id.* at 10). Plaintiffs further argue that OPM's enforcement authority is not exclusive. (*Id.* at 12). Plaintiffs rely on *In re Anthem, Inc. Data Breach Litigation*,

162 F. Supp. 3d 953 (N.D. Cal. 2016) (“*Anthem I*”), asserting that, in that case, the court considered and rejected substantially similar arguments regarding OPM’s exclusive authority to enforce the exact same contract. (*Id.*).

3. Whether Plaintiffs are Intended Third Party Beneficiaries

Plaintiffs are not parties to the Federal BCBSA contract, and as a result, to assert a claim they must establish that they are intended third party beneficiaries of that contract. “According to federal common law, a third party must be an intended, rather than incidental, beneficiary in order to enforce a contract. Federal common law, in deciding whether a third-party beneficiary may sue, looks to the same considerations as does the Restatement of Contracts.” *Caires v. JP Morgan Chase Bank, N.A.*, 880 F. Supp. 2d 288, 301 (D. Conn. 2012) (quotation omitted); *accord Anthem I*, 162 F. Supp. 3d at 1009-10 (following Restatement when evaluating third-party beneficiary claim to enforce the Federal BCBSA Contract). Section 302 of the Restatement (Second) of Contracts defines an “intended beneficiary” as follows:

Unless otherwise agreed between promisor and promisee, a beneficiary of a promise is an intended beneficiary if recognition of a right to performance in the beneficiary is appropriate to effectuate the intention of the parties and . . . (b) the circumstances indicate that the promisee intends to give the beneficiary the benefit of the promised performance.

Restatement (Second) of Contracts § 302(1) (1981); *see also id.* at cmt. a (distinguishing “an ‘intended’ beneficiary, who acquires a right by virtue of a promise, from an ‘incidental’ beneficiary, who does not”). In explaining federal common law, the Second Circuit explained that “[p]roving third-party beneficiary status requires that the contract terms “‘clearly evidence[] an intent to permit enforcement by the third party’ in

question.” *Hillside Metro Assocs., LLC v. JPMorgan Chase Bank, Nat. Ass’n*, 747 F.3d 44, 49 (2d Cir. 2014) (quoting *Premium Mortg. Corp. v. Equifax, Inc.*, 583 F.3d 103, 108 (2d Cir. 2009) (alteration in original) (quoting *Fourth Ocean Putnam Corp. v. Interstate Wrecking Co.*, 66 N.Y.2d 38, 45 (1985))).

The Restatement sets forth a heightened standard for evaluating intended third party beneficiary status where a government agency is a party to the contract. The rationale for this is that “[g]overnment contracts often benefit the public, but individual members of the public *are treated as incidental beneficiaries unless a different intention is manifested.*” Restatement (Second) of Contracts § 313 cmt. a (emphasis added). Section 313 of the Restatement therefore provides:

[A] promisor who contracts with a . . . governmental agency to do an act for or render a service to the public is not subject to contractual liability to a member of the public for consequential damages resulting from performance or failure to perform unless (a) the terms of the promise provide for such liability; or (b) the promisee is subject to liability to the member of the public for the damages and a direct action against the promisor is consistent with the terms of the contract and with the policy of the law authorizing the contract and prescribing remedies for its breach.

“Thus, under the Restatement of Contracts, a plaintiff claiming to be the intended third party beneficiary of a government contract must show that he was intended to benefit from the contract and that third-party beneficiary claims are consistent with the terms of the contract and the policy underlying it.” *Rivera v. Bank of Am. Home Loans*, No. 09 CV 2450 (LB), 2011 WL 1533474, at *4 (E.D.N.Y. Apr. 21, 2011) (quotations omitted).

Despite Plaintiffs’ reliance on *Anthem I*, that court did not address whether the federal employee plaintiffs were intended third party beneficiaries of the Federal BCBSA

contract, given that the defendants did not challenge the plaintiffs' status as such. *See Anthem I*, 162 F. Supp. 3d at 1009 ("Plaintiffs assert—and, more importantly, Defendants do not challenge—the fact that Plaintiffs are intended third party beneficiaries under the Federal BCBSA contract. . . . Thus, at least for purposes of the instant motions to dismiss, Plaintiffs have cleared the first hurdle by demonstrating intended third party beneficiary status."). While *Anthem I* considered—and rejected—the defendants' related argument that the plaintiffs' claims were barred because FEHBA's scheme gives OPM exclusive enforcement authority, that decision offers no analysis of the precise questions at issue here: whether the Federal BCBSA Contract evidences a clear intent to permit enforcement by Plaintiffs, and whether the third-party beneficiary claims are consistent with the terms of the Federal BCBSA Contract.

Regarding the first issue, intent to benefit, Plaintiffs argue that "the entire purpose of the [Federal] BCBSA Contract is to bestow benefits on federal employees enrolled in the FEHB." (Pl. BCBSA Opp. at 9). The Court agrees that the general purpose of the contract is to benefit federal employees. This is plainly evident from the terms of the contract itself. Section 2.2(a) of the Federal BCBSA Contract states that "the [c]arrier shall provide the benefits as described in the agreed upon" Statement of Benefits, which provides that enrollees "are entitled to the benefits described" within it. (Dkt. 111-7 at 5). Thus, despite not being parties to the contract, federal employees are intended to benefit from it. But whether the contract generally benefits those employees does not answer the entire question. As the Second Circuit has instructed, "[p]roving third-party beneficiary status requires that the contract terms clearly evidence an *intent to permit enforcement* by

the third party in question.” *Hillside Metro Assocs.*, 747 F.3d at 49 (emphasis added) (internal quotation marks, citations, and alterations omitted); *see also Caires*, 880 F. Supp. 2d at 302 (“[C]ourts have rejected the contention that a member of the public can be considered a third party beneficiary of a government contract on the sole basis that [the] contract was intended to benefit the public *absent clear intent indicating the public’s right to enforce the contract* as a third party beneficiary.” (emphasis added)).

Plaintiffs’ allegations do not meet this hurdle. In the CMC, they allege, without elaboration, that “[e]nrollees in the Federal BCBS Plan, including the Federal Employee Plaintiffs and Federal Employee Class Members, are the intended beneficiaries of benefits and services under the Federal BCBS Contract, including terms pertaining to the confidentiality of Enrollees’ Personal Information.” (CMC at ¶ 87). In their opposition to BSBCA’s motion, Plaintiffs elaborate on the clear intent requirement. They assert that intent is evident because the contract provides enrollees an enforcement mechanism to dispute “health benefits” claims; however, according to Plaintiffs’ reasoning, enrollees do not have any enforcement mechanism for disputes that do not concern health benefits claims, such as a dispute regarding data security, and, as a result, federal employees should be able to enforce those rights through a breach of contract claim. (Pl. BCBSA Opp. at 9-10). In essence, Plaintiffs argue that they have shown “clear intent” to enforce the contract because it is silent regarding enrollees’ ability to enforce non-health benefits claims. However, silence cannot be interpreted to manifest a clear intent to permit enforcement. Accordingly, the Court grants BCBSA’s motion to dismiss Plaintiffs’ third-party beneficiary claim with prejudice on the basis that the Federal Employee

Plaintiffs are not intended third-party beneficiaries of the Federal BCBSA Contract. Consequently, the Court need not address BCBSA's other asserted grounds for dismissing this claim. (BCBSA Mot. at 14-22).

D. Unjust Enrichment Claim (Seventh Claim for Relief)

In their Seventh Claim, Plaintiffs assert, in the alternative, a claim for unjust enrichment against the Excellus Defendants. (CMC at ¶¶ 254-62). Plaintiffs allege that they “conferred a monetary benefit on Defendants in the form of premiums,” that a portion of those fees “should have been used by Defendants . . . to pay for the administrative costs of reasonable data privacy and security practices and procedures,” and that, “[a]s a result of Defendants’ conduct . . . , Plaintiffs and Class Members suffered actual damages in an amount equal to the difference in value between health insurance and health benefit services associated with the reasonable data privacy and security practices and procedures that Plaintiffs and Class Members paid for, and the inadequate health insurance and health benefits services without reasonable data privacy and security practices and procedures that they received.” (*Id.* at ¶¶ 256-59). According to Plaintiffs, “Defendants should not be permitted to retain money belonging to Plaintiffs and Class Members because Defendants failed to use that money to implement the reasonable data privacy and security practices and procedures that Plaintiffs and Class Members paid for and that were otherwise mandated by HIPAA regulations, federal and state law, and industry standards and best practices.” (*Id.* at ¶ 260).

The Excellus Defendants seek to dismiss Plaintiffs’ unjust enrichment claim, contending that there can be no unjust enrichment claim where an express agreement

governs the same subject matter and they can obtain relief on their breach of contract claim. (Excellus Mot. at 25). Plaintiffs respond that their unjust enrichment claim is pleaded in the alternative, and as a result, “the Court should defer ruling at least until the breach of contract claim is resolved on the merits.” (Pl. Excellus Opp. at 18).

Under New York law, “[a] ‘quasi contract’ only applies in the absence of an express agreement, and is not really a contract at all, but rather a legal obligation imposed in order to prevent a party’s unjust enrichment.” *Clark-Fitzpatrick, Inc. v. Long Island R. Co.*, 70 N.Y.2d 382, 388 (1987). “It is impermissible . . . to seek damages in an action sounding in quasi contract where the suing party has fully performed on a valid written agreement, the existence of which is undisputed, and the scope of which clearly covers the dispute between the parties.” *Id.*; accord *Corsello v. Verizon N.Y., Inc.*, 18 N.Y.3d 777, 790 (2012) (“An unjust enrichment claim is not available where it simply duplicates, or replaces, a conventional contract . . . claim.”).

In *In re Anthem, Inc. Data Breach Litigation*, No. 15-MD-02617-LHK, 2016 WL 3029783 (N.D. Cal. May 27, 2016) (“*Anthem II*”)—a data breach case with facts similar to this one—the court declined to dismiss an unjust enrichment claim based on the assertion that it was duplicative of a breach of contract claim. *Id.* at *28. In so concluding, the *Anthem II* court noted that “New York courts have denied motions to dismiss unjust enrichment claims . . . ‘where there is a bona fide dispute as to the existence of a contract or where the contract does not cover the dispute in issue, plaintiff may proceed upon a theory of quantum meruit and will not be required to elect his or her remedies.’” *Id.* (quoting *Joseph Sternberg, Inc. v. Walber 36th St. Assocs.*, 187 A.D.2d

225, 228 (1st Dep't 1993)). In *Anthem II*, the parties disputed whether the insurance company's privacy policies were incorporated into the contracts with Plaintiffs; this dispute concerning incorporation by reference created ambiguity as to whether the contract covered the dispute at issue. *Id.* Because the contract was ambiguous, it was not clear that the breach of contract claim was duplicative of the unjust enrichment claim, and so the court declined to dismiss the unjust enrichment claim. *Id.*

A similar outcome is warranted here. As noted above, the parties dispute whether the parties have an enforceable contract with definite and material terms regarding the provision of data security. Accordingly, Plaintiffs will neither be required to elect their remedy nor barred from proceeding on an unjust enrichment theory. The Court therefore denies the Excellus Defendants' motion to dismiss the unjust enrichment claim based on their contention that that claim is precluded by the breach of contract claim.

III. Negligent Misrepresentation Claim (Sixth Claim for Relief)

In their Sixth Claim, Plaintiffs assert a claim for negligent misrepresentation against the Excellus Defendants. They allege as follows:

Defendants negligently and recklessly misrepresented material facts pertaining to the sale of insurance and health benefits services by representing . . . that they would maintain adequate data privacy and security practices and procedures to safeguard Plaintiffs and Statewide Class Members' Personal Information from unauthorized disclosure, release, data breaches, and cyber attack . . . [and] that they would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of Plaintiffs and Statewide Class Members' Personal Information.

(CMC at ¶¶ 248-49). Plaintiffs allege that the Excellus Defendants knew or should have known that their representations were not true because they had received warnings about

the inadequacy of their data security. (*Id.* at ¶ 250). Plaintiffs further allege that they relied on the Excellus Defendants’ misrepresentations when purchasing health insurance, but Plaintiffs would not have done so had they known of the Excellus Defendants’ inadequate data security and failure to comply with federal and state laws pertaining to data security. (*Id.* at ¶ 252).

The Excellus Defendants seek dismissal of the negligent misrepresentation claim on two grounds. (Excellus Mot. at 16-19). First, the Excellus Defendants contend that “none of the plaintiffs allege facts supporting the conclusion that they justifiably or reasonably relied on” the Excellus Defendants’ “alleged representations contained in Excellus’s HIPAA privacy notice . . . [and] on privacy policies placed on Excellus’s website related to the use of that site.” (*Id.* at 16-17). Second, the Excellus Defendants contend that “plaintiffs and Excellus did not stand in the special relationship required to give rise to a duty of care under New York law.” (*Id.* at 17).

Federal Rule of Civil Procedure 9(b) requires that “[i]n alleging fraud or mistake, a party must state with particularity the circumstances constituting fraud or mistake. Malice, intent, knowledge, and other conditions of a person’s mind may be alleged generally.” Fed. R. Civ. P. 9(b). Despite a “muddled history in this circuit,” Rule 9(b) applies to negligent misrepresentation claims under New York law. *Schwartzco Enters. LLC v. TMH Mgmt., LLC*, 60 F. Supp. 3d 331, 350 (E.D.N.Y. 2014).

In *Eternity Global Master Fund Ltd. v. Morgan Guaranty Trust Co. of New York*, 375 F.3d 168 (2d Cir. 2004), the Second Circuit declined to hold that Rule 9(b) applied to a state law claim for negligent misrepresentation. *Id.* at 188 (“Rule 9(b) may or may not

apply to a state law claim for negligent misrepresentation. District court decisions in this Circuit have held that the Rule is applicable to such claims, . . . but this Court has not adopted that view, and we see no need to do so here because [the appellant's] claim fails under the liberal pleading standards of Rule 8 and, *a fortiori*, the strictures of Rule 9(b).”). Although “many district courts have proceeded on the assumption that the Second Circuit has not explicitly ruled on whether Rule 9(b) . . . applies to New York negligent misrepresentation claims,” *Schwartzco Enters.*, 60 F. Supp. 3d at 349, the Second Circuit decided the issue following *Eternity Global*.

In *Aetna Casualty & Surety Co. v. Aniero Concrete Co., Inc.*, 404 F.3d 566 (2d Cir. 2005), the Second Circuit held that a negligent misrepresentation claim “must be pled in accordance with the specificity criteria of Rule 9(b).” *Id.* at 583. Accordingly, *Aetna* controls, and Plaintiffs’ negligent misrepresentation claim must withstand Rule 9(b) scrutiny. *See Directv, LLC v. Wright*, No. 15-CV-474-FPG, 2016 WL 3181170, at *9 (W.D.N.Y. June 3, 2016) (“[S]ince negligent misrepresentation is a type of fraud, a party pleading negligent misrepresentation is . . . subject to a heightened pleading standard under Federal Rule of Civil Procedure 9(b).”); *Schwartzco Enters.*, 60 F. Supp. 3d at 350; *BNP Paribas Mortg. Corp. v. Bank of Am., N.A.*, 949 F. Supp. 2d 486, 508 (S.D.N.Y. 2013) (collecting district court cases that apply Rule 9(b) to negligent misrepresentation claims).

Under New York law, “[a] claim for negligent misrepresentation requires the plaintiff to demonstrate (1) the existence of a special or privity-like relationship imposing a duty on the defendant to impart correct information to the plaintiff; (2) that the

information was incorrect; and (3) reasonable reliance on the information.” *J.A.O. Acquisition Corp. v. Stavitsky*, 8 N.Y.3d 144, 148 (2007); accord *King v. Crossland Sav. Bank*, 111 F.3d 251, 258 (2d Cir. 1997) (“[U]nder New York law a cause of action for negligent misrepresentation can be maintained only when the plaintiff *himself or herself* relies on statements made by the *defendant*.” (emphasis in original)).

Reasonable or justifiable reliance is also an element of a negligent misrepresentation claim under any other potentially applicable law. See *Bloch v. Wells Fargo Home Mortg.*, 755 F.3d 886, 890 (11th Cir.) (“Under Florida law, negligent misrepresentation requires: (1) misrepresentation of a material fact; (2) the representor must either know of the misrepresentation, must make the representation without knowledge as to its truth or falsity, or must make the representation under circumstances in which he ought to have known of its falsity; (3) the representor must intend that the representation induce another to act on it; (4) injury must result to the party acting in justifiable reliance on the misrepresentation.” (quotation omitted)), *cert. denied*, 134 S. Ct. 2711 (2014); *Arnesen v. Rivers Edge Golf Club & Plantation, Inc.*, 781 S.E.2d 1, 12 (N.C. 2015) (“The tort of negligent misrepresentation occurs when a party justifiably relies to his detriment on information prepared without reasonable care by one who owed the relying party a duty of care”); *Conroy v. Regents of Univ. of Cal.*, 203 P.3d 1127, 1135 (Cal. 2009) (stating that the “elements of fraud . . . are (1) a misrepresentation, (2) with knowledge of its falsity, (3) with the intent to induce another’s reliance on the misrepresentation, (4) justifiable reliance, and (5) resulting damage”); *McCalment v. Eli Lilly & Co.*, 860 N.E.2d 884, 896 (Ind. Ct. App. 2007) (“Detrimental reliance is also an

element of negligent misrepresentation. . . .”); *Kaufman v. i-Stat Corp.*, 754 A.2d 1188, 1195 (N.J. 2000) (stating that justifiable reliance is an element of negligent misrepresentation); *Bortz v. Noon*, 729 A.2d 555, 561 (Pa. 1999) (“Negligent misrepresentation requires proof of: (1) a misrepresentation of a material fact; (2) made under circumstances in which the misrepresenter ought to have known its falsity; (3) with an intent to induce another to act on it; and; (4) which results in injury to a party acting in justifiable reliance on the misrepresentation.”).

The Excellus Defendants argue that “no plaintiff has alleged facts supporting the conclusion he or she relied on or even knew about the alleged misstatements cited in the complaint.” (Excellus Mot. at 17). According to the Excellus Defendants, Plaintiffs’ assertion that they purchased insurance in reliance on alleged misstatements (CMC at ¶ 251) is conclusory. (Excellus Mot. at 17-18). Plaintiffs respond that their allegations are sufficient to establish reliance under New York law and the law of any other applicable state: the CMC alleges that Plaintiffs were informed that Defendants would adhere to privacy policies and practices (*e.g.*, CMC at ¶¶ 60-90), and purchased insurance in reliance on those misrepresentations (*id.* at ¶¶ 251-52). (Pl. Excellus Opp. at 19).

The Court agrees with the Excellus Defendants. Plaintiffs have failed to allege with any particularity that they actually read or saw the notices concerning privacy policies and practices as described in the CMC at ¶¶ 60-94. Instead, Plaintiffs only offer the conclusory assertion that, “[i]n reliance upon Defendants’ misrepresentations, Plaintiffs and Statewide Class Members purchased insurance or health benefits services from Defendants.” (CMC at ¶ 251). Failure to plead any facts concerning their

purported reliance requires dismissal of Plaintiffs' negligent misrepresentation claim. *See DeBlasio v. Merrill Lynch & Co.*, No. 07 Civ 318(RJS), 2009 WL 2242605, at *24 n.15 (S.D.N.Y. July 27, 2009) (dismissing negligent misrepresentation claim because the plaintiffs failed to allege that they actually read and relied on purported misrepresentations); *Granite Partners, L.P. v. Bear, Stearns & Co.*, 58 F. Supp. 2d 228, 258 (S.D.N.Y. 1999) (finding reliance inadequately pleaded because "[d]espite the [plaintiffs'] catch-all allegation that [they] relied upon [the defendant's] statements . . . , the [plaintiffs] never venture[] to actually plead facts that underlie this reliance"); *see also Tuosto v. Philip Morris USA Inc.*, No. 05 Civ. 9384(PKL), 2007 WL 2398507, at *9 (S.D.N.Y. Aug. 21, 2007) (finding reliance inadequately pleaded because the complaint did "not allege that [the plaintiff] saw . . . any specific . . . advertisement, [but] simply that [the defendant's] advertisements were widely circulated and intended to mislead").

In addition to challenging the reliance requirement, the Excellus Defendants further argue that Plaintiffs' negligent misrepresentation claim under New York law should be dismissed because Plaintiffs have not adequately alleged that they and the Excellus Defendants are in a special relationship. (Excellus Mot. at 18-19). In the CMC, Plaintiffs allege that a special relationship exists between them and Defendants for two reasons:

Defendants entered into a "special relationship" with the Plaintiffs and Class Members whose Personal Information was requested, collected, and received by Defendants. A "special relationship" also exists between Defendants and Plaintiffs and the Class Members because Defendants are insurers and providers of health plan services and thus stand in a fiduciary or quasi-fiduciary relationship with Plaintiffs and Class Members.

(CMC at ¶ 193).

The Excellus Defendants contend that courts applying New York law “consistently reject negligent misrepresentation claims brought against insurers absent some specific allegations of interactions between the parties creating a special relationship.” (*Id.* at 19). Plaintiffs respond that their allegations are sufficient to establish that the Excellus Defendants owed Plaintiffs a duty of care: “Plaintiffs allege they were without knowledge, received assurances from Defendants who had exclusive knowledge, and relied on those assurances.” (Pl. Excellus Opp. at 21 (citing CMC at ¶¶ 167(g), 251-52)).

As stated above, one element of a negligent misrepresentation claim under New York law is “the existence of a special or privity-like relationship imposing a duty on the defendant to impart correct information to the plaintiff.” *J.A.O. Acquisition Corp.*, 8 N.Y.3d at 148; *see also Stewart v. Jackson & Nash*, 976 F.2d 86, 90 (2d Cir. 1992) (“[U]nder New York law, a plaintiff may recover for negligent misrepresentation only where the defendant owes her a fiduciary duty.”). “New York courts do not follow a *per se* rule prohibiting the recognition of a fiduciary relationship in the insurance context, but a plaintiff still must allege facts indicating a relationship closer than arm’s-length.” *Phillips v. Am. Int’l Grp., Inc.*, 498 F. Supp. 2d 690, 695-96 (S.D.N.Y. 2007) (quotation omitted). If the plaintiff makes no showing that its relationship with the defendant “is unique or differs from that of a reasonable consumer,” there is “no reason to depart from the general rule that the relationship between the parties to a contract of insurance is strictly contractual in nature. No special relationship of trust or confidence arises out of

an insurance contract between the insured and the insurer; the relationship is legal rather than equitable.” *Batas v. Prudential Ins. Co. of Am.*, 281 A.D. 2d 260, 264 (1st Dep’t 2001).

Here, the CMC does not include any facts that would suggest that Plaintiffs have a relationship with the Excellus Defendants that is unique or differs from that of a reasonable consumer. Plaintiffs allege that a special relationship existed because the Excellus Defendants had exclusive knowledge about their data security policies, and Plaintiffs provided their personal information and received assurances about the Excellus Defendants’ data security. (CMC at ¶¶ 193, 251-52). Nothing about these interactions would appear to fall outside the scope of what is routine between insurers and insureds, and therefore, the interactions do not suggest any kind of special relationship of trust and confidence.

Accordingly, the Court grants the Excellus Defendants’ motion to dismiss Plaintiffs’ negligent misrepresentation claim on the basis that Plaintiffs have not adequately alleged reliance or a special relationship. Because Plaintiffs could theoretically allege facts to plausibly state a claim for negligent misrepresentation, the dismissal is without prejudice and the Court grants Plaintiffs leave to replead this claim.

IV. Plaintiffs’ State Statutory Claims (Eighth, Ninth, and Tenth Claims for Relief)

In their Eighth, Ninth, and Tenth Claims for relief, Plaintiffs assert violations of various state laws against the Excellus Defendants. (CMC at ¶¶ 263-303). One of those state law claims, under New York General Business Law (“GBL”) § 349, is also asserted

against BCBSA. (BCBSA Mot. at 3-4 (“Plaintiffs’ counsel have informed BCBSA’s counsel that the only state law violation alleged against BCBSA is under GBL § 349, and that Plaintiffs are dropping the remaining portions of Count VIII, and all of Counts IX and X, as against BCBSA.”)).

A. New York General Business Law § 349 (included in Eighth Claim for Relief)

The Excellus Defendants seek dismissal of Plaintiffs’ claim under New York General Business Law (“GBL”) § 349 (Excellus Mot. at 19-24), as does BCBSA (BCBSA Mot. at 22-25). The Court addresses Defendants’ challenges to this claim in turn.

New York Plaintiffs assert a claim under GBL § 349. GBL § 349 prohibits “[d]eceptive acts or practices in the conduct of any business, trade or commerce or in the furnishing of any service.” N.Y. Gen. Bus. § 349(a). To successfully assert a GBL § 349 claim, “a plaintiff must allege that a defendant has engaged in (1) consumer-oriented conduct that is (2) materially misleading and that (3) plaintiff suffered injury as a result of the allegedly deceptive act or practice.” *Orlander v. Staples, Inc.*, 802 F.3d 289, 300 (2d Cir. 2015) (quoting *Koch v. Acker, Merrall & Condit Co.*, 944 N.Y.S.2d 452, 452 (2012)). “[A]n action under § 349 is not subject to the pleading-with-particularity requirements of Rule 9(b), Fed. R. Civ. P., but need only meet the bare-bones notice-pleading requirements of Rule 8(a). . . .” *McCracken v. Verisma Sys., Inc.*, 131 F. Supp. 3d 38, 46 (W.D.N.Y. 2015) (quoting *Pelman ex rel. Pelman v. McDonald’s Corp.*, 396 F.3d 508, 511 (2d Cir. 2005)).

New York Plaintiffs allege that, in the course of their business, Defendants collected and stored Plaintiffs' personal information, and engaged in deceptive practices, as follows. Defendants allegedly:

- misrepresented and advertised that they “would maintain adequate data privacy and security practices and procedures to safeguard New York Class Members’ PII and PHI from unauthorized disclosure, release, data breaches, and cyber attack,” (CMC at ¶ 281(a));
- misrepresented material facts by “representing and advertising that they did and would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of New York Class Members’ PII and PHI,” (*id.* at ¶ 281(b));
- “omitted, suppressed, and concealed the material fact of the inadequacy of their privacy and security protections for New York Class Members’ PII and PHI,” (*id.* at ¶ 281(c));
- failed “to maintain the privacy and security of New York Class Members’ PII and PHI, in violation of duties imposed by and public policies reflected in applicable federal and state laws . . . ,” (*id.* at ¶ 281(d));
- failed “to disclose the Excellus data breach to New York Class Members in a timely and accurate manner,” (*id.* at ¶ 281(e)); and
- failed “to take proper action following the Excellus data breach to enact adequate privacy and security measures and protect New York Class Members’ PII and PHI from further unauthorized disclosure, release, data breaches, and theft,” (*id.* at ¶ 281(f)).

1. Material Misrepresentation

The Excellus Defendants argue, with respect to the second element of a GBL § 349 claim, that Plaintiffs have not alleged a materially misleading statement attributable to Defendants. (Excellus Mot. at 20-21). Relying primarily on *Abdale v. North Shore-Long Island Jewish Health System, Inc.*, 49 Misc. 3d 1027 (S. Ct. Queens Cty. 2015), the

Excellus Defendants argue that Plaintiffs have not identified any specific statements in the data privacy and security practices and procedures that provided Plaintiffs an unlimited guarantee that their data could not be stolen. (*Id.* at 20). Thus, the Excellus Defendants contend that there can be no plausible allegation that they engaged in a misleading act, defeating Plaintiffs' claim under GBL § 349. (*Id.* at 20-21).

In opposition, Plaintiffs contend that the CMC alleges that the Defendants violated GBL § 349 in two ways, both of which are actionable under that statute: (1) by omission—that is, by “neglecting to disclose their inadequate cybersecurity practices”; and (2) by affirmative misrepresentation of their efforts to safeguard Plaintiffs' personal information. (Pl. Excellus Opp. at 22). Plaintiffs point to *Anthem I*, 162 F. Supp. 3d at 991-97, in which the court concluded that the plaintiffs adequately pleaded their GBL § 349 claim. According to Plaintiffs, “Anthem, like Defendants here, made [misleading] representations in statements on its websites and in the privacy notices it provided its customers.” (*Id.*). Plaintiffs attempt to distinguish *Abdale*, arguing that, in that case, the court applied an “unlimited guaranty” standard that “is not the law”; Plaintiffs argue that the relevant inquiry, under New York law, is whether the act is likely to mislead a reasonable consumer acting reasonably under the circumstances. (*Id.* at 22 n.19).

New York courts define “deceptive acts and practices” objectively as “representations or omissions, limited to those likely to mislead a reasonable consumer acting reasonably under the circumstances.” *Oswego Laborers' Local 214 Pension Fund v. Marine Midland Bank, N.A.*, 85 N.Y.2d 20, 26 (1995). Claims based on omissions are cognizable “where the business alone possesses material information that is relevant to

the consumer and fails to provide this information.” *Id.* Whether a particular act or practice is deceptive is usually a factual question. *See Quinn v. Walgreen Co.*, 958 F. Supp. 2d 533, 543 (S.D.N.Y. 2013) (citing *Sims v. First Consumers Nat. Bank*, 303 A.D.2d 288, 289 (1st Dep’t 2003)); *see also Buonasera v. Honest Co., Inc.*, No. 16 Civ. 1125 (VM), 2016 WL 5812589, at *8 (S.D.N.Y. Sept. 23, 2016) (“Courts have generally held that since this second factor requires a reasonableness analysis, it cannot be resolved on a motion to dismiss.”).

In *Anthem I*, the court concluded that the plaintiffs adequately pleaded a GBL § 349 claim. *See* 162 F. Supp. 3d at 997. In reaching that conclusion, the *Anthem I* court rejected the defendants’ challenges “that [the] [p]laintiffs’ claim is based on a private contract dispute, and is therefore not the result of consumer-oriented conduct” and “that [the] [p]laintiffs ha[d] failed to demonstrate actual harm and causation.” *Id.* at 991. The *Anthem I* court concluded that the plaintiffs’ claims satisfied the GBL’s consumer-oriented requirement, that some of the alleged harms constituted cognizable injuries under GBL § 349, and that they had adequately alleged causation for purposes of a GBL § 349 claim. *Id.* at 992-97. The defendants in that case did not raise any challenge to the second prong of a GBL § 349 claim, that is, the “materially misleading” requirement that the Excellus Defendants challenge here. *See id.* As a result, the *Anthem I* court’s analysis of this claim is not particularly informative.

In *Abdale*, 49 Misc. 3d at 1030, patients sued medical facilities in New York state court after their personal information was stolen in a data breach. The patients asserted a claim under GBL § 349, alleging that the medical facilities maintained a privacy policy

that guaranteed that the patients' personal information would not be released to unauthorized third parties without the patients' consent, and that the facilities' failure to protect their information such that the breach occurred contravened their privacy policy and constituted a deceptive and unlawful practice. *Id.* at 1038-39. The *Abdale* court dismissed the claim, concluding that:

the statements allegedly made by defendants in the privacy policy and online notices do not constitute an unlimited guaranty that patient information could not be stolen or that computerized data could not be hacked. [The] [d]efendants' alleged failure to safeguard [the] plaintiffs' protected health information and identifying information from theft did not mislead the plaintiffs in any material way and does not constitute a deceptive practice within the meaning of [GBL § 349].

Id. at 1039. As Plaintiffs point out, however, the *Abdale* court did not discuss how "a reasonable consumer acting reasonably under the circumstances" would view the statements in the privacy policy and online notices that were at issue in that case. Thus, the *Abdale* court's thinly-reasoned analysis is not persuasive.

In light of the foregoing, the Court disagrees with the Excellus Defendants. Based on Plaintiffs' allegations, it is at least plausible that the Excellus Defendants' representations in their privacy policies and on their websites concerning data security (catalogued above) would lead a reasonable consumer to believe that the Excellus Defendants were providing more adequate data security than they purportedly were. (CMC at ¶ 281). It is also at least plausible that the Excellus Defendants' failure to disclose the purportedly inadequate data security measures would mislead a reasonable consumer. (*See id.*). At least at the pleading stage, these allegations are sufficient. Indeed, at least one district court has held, in a data breach case, that the plaintiffs

sufficiently alleged materially misleading conduct based on the allegation that the defendants misrepresented that they “would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of” New York class members’ personal information. *In re Experian Data Breach Litig.*, No. SACV 15-1592 AG (DFMx), 2016 WL 7973595, at *5 (C.D. Cal. Dec. 29, 2016). Plaintiffs’ CMC contains a nearly identical allegation. (CMC at ¶ 281(b)). And, given that “whether a particular act or practice is deceptive is usually a question of fact,” *Quinn*, 958 F. Supp. 2d at 543, the Court declines to conclude as a matter of law that the Excellus Defendants’ purported deceptive representations and omissions are not misleading to a reasonable consumer. Accordingly, the Court declines to dismiss the GBL § 349 claim on the ground that Plaintiffs have not alleged a materially misleading statement.

2. Whether violations of other statutes support a claim under GBL § 349

The Excellus Defendants also argue that Plaintiffs have used GBL § 349 to allege liability under other statutes that do not provide for a private right of action: the Federal Trade Commission Act (15 U.S.C. § 45), HIPAA (42 U.S.C. § 1302d), the Gramm-Leach-Bliley Act (15 U.S.C. § 6801), New York’s Protection Mechanisms for Insurance Payment Information (N.Y. Soc. Serv. § 367-a(2)(B)), and N.Y. GBL § 899-aa(2). (Excellus Mot. at 21-22). Plaintiffs respond only briefly in a footnote, arguing that “Plaintiffs allege that Defendants violated § 349 itself by engaging in consumer-oriented conduct that was materially misleading, thereby injuring Plaintiffs.” (Pl. Excellus Opp. at 23 n.20).

The Excellus Defendants’ argument primarily relies on *Conboy v. AT & T Corp.*, 84 F. Supp. 2d 492 (S.D.N.Y. 2000), *aff’d*, 241 F.3d 242 (2d Cir. 2001). In that case, the district court dismissed the plaintiff’s claim that the defendant engaged in a deceptive act, within the meaning of GBL § 349, by violating GBL § 601(6), which prohibits a creditor from communicating with a debtor in a manner that could be expected to harass the debtor. *Id.* at 506. The district court noted that GBL § 601(6) does not supply a private cause of action, and as a result, plaintiffs could not thwart legislative intent not to allow private enforcement of GBL § 601(6) by casting a GBL § 601(6) claim as a GBL § 349 claim. *Id.* This holding was affirmed on appeal. *Conboy*, 241 F.3d at 257-58.

As the Excellus Defendants point out, none of the statutes cited in the CMC at ¶ 281(d) or (e) provide a private right of action. *See Alfred Dunhill Ltd. v. Interstate Cigar Co.*, 499 F.2d 232, 237 (2d Cir. 1974) (“[T]he provisions of the Federal Trade Commission Act may be enforced only by the Federal Trade Commission. Nowhere does the Act bestow upon either competitors or consumers standing to enforce its provisions.”); *Cassidy v. Nicolo*, No. 03-CV-6603-CJS, 2005 WL 3334523, at *5 (W.D.N.Y. Dec. 7, 2005) (collecting cases holding that HIPAA does not authorize a private right of action); *Wood v. Greenberry Fin. Servs., Inc.*, 907 F. Supp. 2d 1165, 1186 (D. Haw. 2012) (holding that the Gramm–Leach–Bliley Act does not provide for a private right of action), *abrogated on other grounds by Compton v. Countrywide Fin. Corp.*, 761 F.3d 1046 (9th Cir. 2014); *Green v. City of N.Y.*, 438 F. Supp. 2d 111, 124 (E.D.N.Y. 2006) (“[T]here is no private right of action under N.Y. Social Services Law § 367–

a(2)(b).”); *Abdale*, 49 Misc. 3d at 1036 (concluding that N.Y. GBL § 899-a provides no private right of action).

Based on the foregoing, the Court dismisses Plaintiffs’ GBL § 349 claims, to the extent that they rest on ¶¶ 281(d) and (e) of the CMC, which use GBL § 349 to allege violations of statutes that do not authorize a private right of action. (CMC at ¶¶ 281(d), (e)). The Excellus Defendants’ motion is granted in this regard and those claims are dismissed with prejudice.

3. GBL § 349 Claim against BCBSA

Plaintiffs’ GBL § 349 claim is asserted against BCBSA in addition to the Excellus Defendants. (*See* BCBSA Mot. at 3-4). BCBSA argues that the claim against it should be dismissed for three reasons: (1) Plaintiffs allege no conduct by BCBSA specifically that could support a GBL § 349 claim against BCBSA, particularly given that the cyberattack occurred on the Excellus Defendants’ information systems, not BCBSA’s information systems; (2) Plaintiffs’ GBL § 349 claim is conflict preempted as applied to the Service Benefit Plan; and (3) the filed rate doctrine bars these claims. The Court addresses each of these arguments in turn.

i. Allegations Specific to BCBSA

As to BCBSA’s first challenge, Plaintiffs respond that, “when read as a whole, the [CMC] describes how BCBSA violated the GBL in the manner described in Count VIII.”⁶ (Pl. BCBSA Opp. at 20). They point to the CMC’s factual allegations that

⁶ As stated above, Plaintiffs’ eighth claim for relief asserts violations of state consumer protection laws, including GBL § 349.

BCBSA distributed to Federal Employee Plaintiffs the Statement of Benefits, which contains a specific promise to keep information confidential and incorporates the Notice of Privacy Policy, which contains representations regarding data security. (*Id.* (citing CMC at ¶¶ 85, 91-92, 281(a)-(d)).

The Court agrees with Plaintiffs that these allegations are sufficiently specific to BCBSA as opposed to any other defendant. As with the GBL § 349 claims against the Excellus Defendants, the various representations by BCBSA that the personal information of Plaintiffs would be protected may plausibly mislead a reasonable consumer. Drawing all reasonable inferences in Plaintiffs' favor, these allegations are sufficiently specific at least at the pleading stage. Accordingly, the Court declines to dismiss Plaintiffs' GBL § 349 claim against BCBSA on this basis.

ii. Conflict Preemption

Conflict preemption applies “where local law conflicts with federal law such that it is impossible for a party to comply with both or the local law is an obstacle to the achievement of federal objectives.” *New York SMSA Ltd. P'ship v. Town of Clarkstown*, 612 F.3d 97, 103-04 (2d Cir. 2010). Where a state law conflicts with a federal law, it is “without effect.” *Id.*

BCBSA's second challenge is that the GBL § 349 claim is conflict preempted as applied to the Service Benefit Plain. (BCBSA Mot. at 24). BCBSA contends that “the broad enforcement powers that Congress gave to OPM, *see, e.g.*, 5 U.S.C. §§ 8902(e), 8910, 8913(a), conflict with Plaintiffs' attempt to use state law to regulate the conduct of a FEHBA carrier.” (*Id.*). BCBSA analogizes this case to *Kight v. Kaiser Foundation*

Health Plan of Mid-Atlantic States, Inc., 34 F. Supp. 2d 334 (E.D. Va. 1999), in which the district court observed that “Congress already adopted an enforcement scheme in FEHBA whereby it delegated the power to police the administration of FEHBA plans to OPM,” and therefore concluded that the plaintiff’s “attempt to seek state law review of Plan administrative policies directly conflicts with the OPM powers.” *Id.* at 342. Those preempted state law claims were for negligence, tortious interference with a contract, and fraud against a FEHBA-governed health plan for creating financial incentives that resulted in doctors providing a reduced standard of healthcare to patients. *Id.* at 341-42. BCBSA argues that a similar result is warranted here where “OPM’s regulations (and the contract terms) give OPM the authority over the very sorts of data security and deceptive advertising allegations Plaintiffs make in their NYGBL § 349 claim.” (BCBSA Mot. at 24 & n.12 (citing regulations that allow OPM to ensure truthfulness of carrier’s marketing materials)).

Plaintiffs point to *Anthem I*, in which the district court rejected a similar conflict preemption-based argument “that the application of certain state laws, including a California consumer protection statute would ‘interfere with OPM’s exclusive authority to police FEHBA carriers.’” (Pl. Reply at 22 (quoting *Anthem I*, 162 F. Supp. 3d at 1015)). In reaching that conclusion, the *Anthem I* court found that “OPM’s exclusive authority does not apply to claims over an individual’s data privacy,” given that FEHBA has a unique federal interest in the provision of health benefits, not data security. *Anthem I*, 162 F. Supp. 3d at 1015. The *Anthem I* court reviewed the Congressional purpose behind FEHBA:

A report from the House of Representatives, for instance, “expressed fear that the imposition of state-law requirements on FEHBA contracts would result in . . . a lack of uniformity of benefits for enrollees in the same plan.” *Helfrich*, 804 F.3d at 1106 (quoting H.R. Rep. No. 95-282 at 4 (1977)) (alteration omitted) (emphasis added). Additional reports from the House and Senate further confirm the importance of FEHBA in the administration of benefits and medical coverage. *See id.* at 1106–07 (citing additional reports).

Id.

The Court finds *Anthem I* to be the more persuasive analogy. *Kight* concerned a health benefits dispute, whereas *Anthem I* concerned the provision of data security and thus is the more analogous case. Accordingly, as the *Anthem I* court concluded, the purpose of FEHBA does not, as a matter of law, evidence an intent to preempt state law claims arising out of promises concerning data security, and as a result, the Court declines to dismiss Plaintiffs’ GBL § 349 claims on the basis of preemption.

iii. Filed Rate Doctrine

In their GBL § 349 claim, one form of damages that Plaintiffs seek is benefit of the bargain damages. (CMC at ¶ 284 (“As a direct and proximate result of Defendants’ deceptive trade practices, New York Class Members suffered injury and/or damages, including the loss of their legally protected interest in the confidentiality and privacy of their PII and PHI, and the loss of the benefit of their respective bargains.”)). BCBSA argues that this cause of action violates the filed rate doctrine.

The filed rate doctrine “holds that any ‘filed rate’—that is, one approved by the governing regulatory agency—is per se reasonable and unassailable in judicial proceedings brought by ratepayers.” *Simon v. KeySpan Corp.*, 694 F.3d 196, 204 (2d Cir.

2012). The doctrine is animated by two concerns: “(1) it protects against discrimination in rates as between different ratepayers, and (2) it prevents courts from having to determine the reasonableness of rates, a task better suited to regulatory agencies.” *Dolan v. Fid. Nat. Title Ins. Co.*, 365 F. App’x 271, 273 (2d Cir. 2010) (citing *Wegoland Ltd. v. NYNEX Corp.*, 27 F.3d 17, 19 (2d Cir. 1994)). The doctrine has been applied strictly:

When the filed rate doctrine applies, it is rigid and unforgiving. Indeed, some have argued that it is unjust. It does not depend on the culpability of the defendant’s conduct or the possibility of inequitable results, nor is it affected by the nature of the cause of action the plaintiff seeks to bring. It applies whenever a claim would implicate its underlying twin principles of preventing carriers from engaging in price discrimination as between ratepayers and preserving the exclusive role of federal agencies in approving rates. And when the doctrine applies, it bars both state and federal claims.

Simon., 694 F.3d at 205 (internal quotation marks and citations omitted).

This doctrine has been applied in the insurance context. Most relevant to this case, in *Anthem II*, the district court concluded that the filed-rate doctrine under New Jersey law foreclosed claims for benefit-of-the-bargain losses in the context of a breach of contract claim. 2016 WL 3029783, at *23-24. Although the *Anthem II* court was applying a state-law version of the filed-rate doctrine, that court observed that the doctrine originated in federal law. *Id.* at *23. The *Anthem II* court concluded that “Plaintiffs’ request for Benefit of the Bargain Losses naturally represents a refund for the portion of Plaintiffs’ premiums that should have, but did not, go towards data security” and thus amounted to an impermissible attempt to “enforce a rate other than the filed rate.” *Id.*

Here, BCBSA argues that the filed-rate doctrine bars Plaintiffs' GBL § 349 claim against it because "awarding damages under that statute would implicate the same nonjusticiability and nondiscrimination principles" underlying the filed-rate doctrine. (BCBSA Mot. at 20-22, 25). That is, according to BCBSA, awarding benefit-of-the-bargain losses would invite the Court to second-guess the insurance premium rates set by OPM and determine what rates were reasonable in light of the purportedly inadequate services. (*Id.* at 21, 25).

The Court agrees. By asking for benefit-of-the-bargain losses, the Court would be in a position of determining the reasonableness of the rates approved by OPM in light of the data breach. Thus, the filed rate doctrine applies such that Plaintiffs may not recover benefit-of-the-bargain damages under their GBL § 349 claim against BCBSA.

Plaintiffs' arguments to the contrary are unpersuasive. They argue that the filed-rate doctrine does not apply because "there is no 'filed rate' at issue. . . ." (Pl. BCBSA Opp. at 17-19, 23). According to Plaintiffs, "the doctrine applies only to rates filed pursuant to statutory filing requirements," and the "Second Circuit has recognized that because the rates in FEHBA contracts are privately negotiated between OPM and private carriers, they are not tariffs, meaning they are not 'filed rates,' and thus the filed rate doctrine does not apply." (*Id.* at 17 (citing *Empire HealthChoice Assurance, Inc. v. McVeigh*, 396 F.3d 136, 144 (2d Cir. 2005), *aff'd on other grounds*, 547 U.S. 677 (2006))). Plaintiffs' reliance on *McVeigh* is misguided. In that case, the Second Circuit observed that, "[u]nder FEHBA, the government does not impose contract terms as it would impose a law. Rather, the OPM negotiates the contract terms privately with

insurance providers.” *McVeigh*, 396 F.3d at 144. But *McVeigh* contains no discussion of the filed rate doctrine; rather, the focus of that case was whether there was subject matter jurisdiction. *Id.* at 138-39. Given that the Second Circuit has defined a “filed rate” as “one approved by the governing regulatory agency,” *Simon*, 694 F.3d at 204, and that OPM is in the position of negotiating and setting insurance premium rates, *see* 5 U.S.C. § 8902(i), the Court is not persuaded by Plaintiffs’ arguments. Accordingly, to the extent that the GBL § 349 claim against BCBSA seeks benefit-of-the bargain losses, it is foreclosed under the filed rate doctrine.⁷

B. California Customer Records Act Claim (Ninth Claim for Relief)

In the ninth claim for relief, the California Plaintiffs assert a violation of the California Customer Records Act (“CCRA”), Cal Civ. Code §§ 1798.80 *et seq.*, against the Excellus Defendants. (CMC at ¶¶ 304-10). California Plaintiffs allege that “Defendants are businesses that own, maintain, and license personal information, within the meaning of [§] 1798.81.5, about Plaintiffs and California Class Members,” (*id.* at ¶ 307), and that “[t]hose Defendants that are not ‘a provider of health care, health care service plan, or contractor regulated by the Confidentiality of Medical Information Act,’ violated Civil Code section 1798.81.5 by failing to implement reasonable measures to protect Plaintiffs’ and California Class Members’ Personal Information,” (*id.* at ¶ 308).

The Excellus Defendants seek dismissal of this claim, arguing that the CCRA does not apply to entities, like Excellus, that are covered under HIPAA. (Excellus Mot. at 22-

⁷ Given that benefit-of-the-bargain losses are not the only damage theories proffered by Plaintiffs in support of the GBL § 349 claim (CMC ¶ 287), the Court does not dismiss this claim in its entirety.

23). Plaintiffs agree that this exception applies and consent to dismissal of this claim against Excellus. (Pl. Excellus Opp. at 26).

The Excellus Defendants also seek dismissal of this claim on the grounds that the CCRA “also does not apply to a ‘health care service plan,’ as defined in the Knox-Keene Health Care Service Plan Act of 1975.” (Excellus Mot. at 22-23). The Excellus Defendants point to those portions of the CMC in which Plaintiffs allege that all defendants are insurance institutions. (*Id.* at 23 (citing CMC at ¶¶ 313, 321)). In their opposition papers, California Plaintiffs note that they “also assert a CCRA claim against Defendant Lifetime Healthcare, Inc.” (Pl. Excellus Opp. at 26). California Plaintiffs contend that “Defendant Lifetime does not fall within the HIPAA exception to the CCRA, and Defendants do not argue otherwise.” (*Id.*).

As an initial matter, California Plaintiffs have failed to respond to the Excellus Defendants’ assertion concerning the applicability of the CCRA to “health care service plans.” (*See id.*; Excellus Reply at 17 n.3). As discussed previously, “courts in this circuit have held that a plaintiff’s failure to respond to contentions raised in a motion to dismiss constitutes an abandonment of the applicable claims.” *Bond*, 2015 WL 5719706, at *8. However, the Second Circuit has also instructed that “the sufficiency of a complaint is a matter of law that the court is capable of determining based on its own reading of the pleading and knowledge of the law. If a complaint is sufficient to state a claim on which relief can be granted, the plaintiff’s failure to respond to a Rule 12(b)(6) motion does not warrant dismissal.” *McCall v. Pataki*, 232 F.3d 321, 322-23 (2d Cir. 2000); *accord Thousand v. Wrest*, No. 14-CV-06616-CJS, 2016 WL 3477242, at *16

(W.D.N.Y. June 27, 2016). Accordingly, the Court considers the merits of California Plaintiffs' CCRA claim against Lifetime, the remaining defendant named in this claim.

The CCRA does not apply to "[a] provider of health care, health care service plan, or contractor regulated by the Confidentiality of Medical Information Act." Cal. Civ. Code § 1798.81.5(e)(1). Under the Confidentiality of Medical Information Act, a "health care service plan" is "any entity regulated pursuant to the Knox-Keene Health Care Service Plan Act of 1975." *Id.* § 56.05(g). The Knox-Keene Health Care Service Plan Act of 1975, in turn, defines a "health care service plan" in two ways:

(1) Any person who undertakes to arrange for the provision of health care services to subscribers or enrollees, or to pay for or to reimburse any part of the cost for those services, in return for a prepaid or periodic charge paid by or on behalf of the subscribers or enrollees.

(2) Any person, whether located within or outside of this state, who solicits or contracts with a subscriber or enrollee in this state to pay for or reimburse any part of the cost of, or who undertakes to arrange or arranges for, the provision of health care services that are to be provided wholly or in part in a foreign country in return for a prepaid or periodic charge paid by or on behalf of the subscriber or enrollee.

Cal. Health & Safety Code § 1345(f).

California Plaintiffs' CCRA claim must be dismissed for two reasons. First, Plaintiffs purport to assert this claim against "[t]hose Defendants that are not 'a provider of health care, health care service plan, or contractor regulated by the Confidentiality of Medical Information Act,'" without specifying which Defendants fall within the exclusions that Plaintiffs identify. (*See* CMC at ¶ 380). Defendants should not have to guess whether this claim is alleged against them. Second, even if this claim could be read as being asserted against Lifetime (as Plaintiffs contend in their opposition papers),

Plaintiffs’ assertions concerning Lifetime undermine that claim. As alleged in the CMC, Lifetime Healthcare “is the parent and/or holding company of a \$6.6 billion family of companies, known as The Lifetime Healthcare Companies, that finances and delivers health care in New York State, as well as long-term care nationwide.” (CMC at ¶ 42). Elsewhere in the CMC, Plaintiffs allege that all Defendants are “insurance institutions” as that term is defined under both New Jersey and North Carolina law. (*Id.* at ¶¶ 313, 320). In other words, Plaintiffs’ own allegations define Lifetime as a “health care service plan.” Accordingly, the Court grants the Excellus Defendants’ motion to dismiss the CCRA claim with prejudice, and leave to replead is denied as futile.

C. New Jersey Insurance Information Practices Act and North Carolina Consumer and Customer Information Privacy Act Claims (Tenth Claim for Relief)

The New Jersey Insurance Information Practices Act (“NJIIPA”) states that “[a]n insurance institution, agent or insurance-support organization shall not *disclose* any personal or privileged information about an individual collected or received in connection with an insurance transaction unless the *disclosure*” falls under one of several enumerated exceptions. N.J. Stat. Ann. § 17:23A-13 (emphasis added). The North Carolina Consumer and Customer Information Privacy Act (“NCCIPA”) mirrors the NJIIPA, stating that “[a]n insurance institution, agent, or insurance-support organization shall not *disclose* any personal or privileged information about an individual collected or received in connection with an insurance transaction unless the *disclosure*” falls under one of several enumerated exceptions. N.C. Gen. Stat. Ann. § 58-39-75 (emphasis added).

In their tenth claim for relief, New Jersey Plaintiffs assert claims against the Excellus Defendants under the NJIIPA, alleging that “Defendants disclosed ‘personal information’ regarding Plaintiffs and members of the New Jersey Class that was collected or received in connection with insurance transactions without the Plaintiffs’ and New Jersey Class Members’ written authorization, in violation of N.J. Stat. § 17:23A-13.” (CMC at ¶ 315). Similarly, North Carolina Plaintiffs assert claims against the Excellus Defendants under the NCCIPA, alleging that “Defendants disclosed personal information regarding Plaintiffs and members of the North Carolina Class that was collected or received in connection with insurance transactions without the Plaintiffs’ and North Carolina Class Members’ written authorization, in violation of N.C. Gen. Stat. § 58-39-75.” (*Id.* at ¶ 323).

The Excellus Defendants seek dismissal of both claims, arguing that neither statute applies because “Excellus did not disclose plaintiffs’ personal information. Rather, cyberattackers hacked into Excellus’s data network systems and may have stolen this information.” (Excellus Mot. at 23). Plaintiffs disagree, arguing that both the NJIIPA and the NCCIPA “protect Plaintiffs from the unauthorized disclosure of confidential information collected by insurance companies during insurance transactions.” (Pl. Excellus Opp. at 24).

Neither the NJIIPA nor the NCCIPA specifically define the terms “disclose” or “disclosure.” *See* N.J. Stat. Ann. § 17:23A-2 (setting forth NJIIPA definitions); N.C. Gen. Stat. Ann. § 58-39-15 (setting forth NCCIPA definitions). The parties have not

identified cases interpreting those terms under either the NJIIPA or the NCCIPA, and this Court's research reveals none.

To support their argument, the Excellus Defendants cite to *Anthem I*, 162 F. Supp. 3d at 1003. (Excellus Mot. at 23). In that case, the district court dismissed a claim under the Georgia Insurance Information and Privacy Protection Act, finding that the plaintiffs had not alleged that the Anthem defendants "disclosed" their personal data, as required for a violation of that statute. The issue was whether the Georgia statute, which prohibited the unlawful disclosure of personal information, applied to the theft of personal information. After examining the text of the statute and relevant case law regarding the meaning of "disclosure," the *Anthem I* court concluded that the Georgia statute did not apply to the theft of personal information. The *Anthem I* court reasoned that, "in order to 'disclose' something, the information holder must commit some affirmative, voluntary act," but such allegations were missing from the plaintiffs' complaint, which alleged only that their personal information was stolen. *Anthem I*, 162 F. Supp. 3d at 1003.

The *Anthem I* court's analysis relied in part on a case cited by the Excellus Defendants: *Galaria v. Nationwide Mutual Ins. Co.*, 998 F. Supp. 2d 646, 662 (S.D. Ohio 2014), *overruled on other grounds*, No. 15-3386, 2016 WL 4728027, at *2 (6th Cir. Sept. 12, 2016) (noting that the plaintiffs did "not appeal the dismissal of their invasion-of-privacy claim"). *Anthem I*, 162 F. Supp. 3d at 1004 (Excellus Mot. at 23-24). In *Galaria*, the district court dismissed a common law invasion of privacy claim because "the Complaint allege[d] the PII was stolen from [Nationwide], not that [Nationwide]

disseminated it to anyone.” 998 F. Supp. 2d at 662. As in *Anthem I*, the district court in *Galaria* distinguished between the theft of personal information and the disclosure of personal information. *Id.*

The Court finds the Excellus Defendants’ arguments persuasive and concludes that the *Anthem I* court’s reasoning concerning the Georgia privacy statute applies with equal force to this case. The Georgia statute at issue in *Anthem I* is nearly identical to the NJIIPA and NCCIPA. Compare N.J. Stat. § 17:23A-13, and N.C. Gen. Stat. Ann. § 58-39-75, with Ga. Code. Ann. § 33-39-14. As the *Anthem I* court observed, dictionary definitions “suggest that, in order to ‘disclose’ something, the information holder must commit some affirmative, voluntary act.” *Anthem I*, 162 F. Supp. 3d at 1002-03 (citations omitted). And as in *Anthem I*, the structure of both the NJIIPA and NCCIPA support the conclusion that disclosure does not encompass a theft; with respect to both of those statutes, the enumerated exceptions to the prohibition against disclosure all involve the holder of personal information affirmatively acting to provide the personal information to a third party. See *id.*; see also N.J. Stat. § 17:23A-13; N.C. Gen. Stat. Ann. § 58-39-75. Finally, as the *Anthem* court observed, a survey of how the term “disclosure” has been defined in other statutes and interpreted by other courts reveals that theft is distinguishable from disclosure. *Anthem I*, 162 F. Supp. 3d at 1003-05.

Plaintiffs offer no persuasive reason why this Court should reach a different conclusion than the *Anthem* court regarding these claims under state privacy statutes. In opposition, Plaintiffs argue that *Anthem* is distinguishable because the Georgia statute at issue in that case prohibits the willful and knowing disclosure of personal information,

see Anthem II, 2016 WL 3029783, at *40, whereas the NJIIPA and NCCIPA have no scienter requirement. (Pl. Excellus Opp. at 25). Plaintiffs' argument is unpersuasive. Like the Georgia statute, the NJIIPA and NCCIPA prohibit intentional disclosure of personal information, not negligent or unintentional disclosure. *Compare* N.J. Stat. Ann. § 17:23A-21 ("No cause of action in the nature of . . . negligence shall arise against any person for disclosing personal or privileged information in accordance with this act . . . [p]rovided, however, this section shall provide no immunity for disclosing or furnishing false information with malice or willful intent to injure any person."), *and* N.C. Gen. Stat. Ann. § 58-39-110 ("No cause of action in the nature of . . . negligence shall arise against any person for disclosing personal or privileged information in accordance with this Article . . . except this section shall provide no immunity for disclosing or furnishing false information with malice or willful intent to injure any person."), *with* Ga. Code Ann. § 33-39-22 ("No cause of action in the nature of . . . negligence shall arise against any person for disclosing personal or privileged information in accordance with this chapter, . . . ; provided, however, this Code section shall provide no immunity for disclosing or furnishing false information with malice or willful intent to injure any person."); *see also Anthem II*, 2016 WL 3029783, at *40 ("The [Georgia statute] does not punish negligent, unintentional conduct; it punishes willful, intentional conduct.").

Plaintiffs further argue that "[t]he term 'disclose,' as used in [the NJIIPA and NCCIPA], must include Defendants' negligent, and even knowing, release of PII and PHI to unauthorized individuals." (Pl. Excellus Opp. at 25). However, the cases cited by Plaintiffs in support of this argument are distinguishable from the facts of this case. Two

cases cited by Plaintiffs involve affirmative acts of revealing personal information. *See Travelers Indem. Co. of Am. v. Portal Healthcare Sols., LLC*, 35 F. Supp. 3d 765, 772 (E.D. Va. 2014) (finding that a disclosure occurred when the defendant had posted medical records online to the public at large), *aff'd sub nom. Travelers Indem. Co. of Am. v. Portal Healthcare Solutions, L.L.C.*, 644 F. App'x 245 (4th Cir. 2016); *Capers v. FedEx Ground*, No. 2:02-CV-5352 (WJM), 2012 WL 2050247, at *5 (D.N.J. June 6, 2012) (finding that the plaintiffs sufficiently alleged a public disclosure of private facts when the defendants posted the plaintiffs' paychecks in locations that allowed them to be viewed by unspecified third parties).

In the third cited case, *Shames-Yeakel v. Citizens Financial Bank*, 677 F. Supp. 2d 994 (N.D. Ill. 2009), the district court, addressing an Indiana common law negligence claim, observed that a bank has a duty not to disclose customers' information, and that "[i]f this duty not to disclose customer information is to have any weight in the age of online banking, then banks must certainly employ sufficient security measures to protect their customers' online accounts." *Id.* at 1008. Like Plaintiffs in this case, the plaintiffs in *Anthem I* cited this case in opposition to the Anthem Defendants' motion to dismiss their claim under the Georgia privacy statute. 162 F. Supp. 3d 953, 1004-05. The *Anthem I* court found *Shames-Yeakel* "ultimately inapposite." *Id.* at 1005. The *Anthem I* court observed that the conclusion in *Shames-Yeakel*—that private plaintiffs may assert a claim under Indiana law for negligence for injuries arising out of a data breach—is "in tension with" a Seventh Circuit decision, *Pisciotta*, 499 F.3d at 640, which held that such a claim is not cognizable under Indiana law. *Anthem I*, 162 F. Supp. 3d at 1005. The

Anthem I court also noted that the *Shames-Yeakel* court concluded that a bank's duty not to disclose encompasses a duty to protect customers' personal information without discussing, referencing, or citing to any supporting authority; moreover, that proposition has not been cited favorably by any federal or state court. *Id.* For the same reasons as the *Anthem I* court, this Court finds Plaintiffs' reliance on *Shames-Yeakel* unpersuasive.

In sum, for the reasons set forth above, the Court concludes that Plaintiffs have failed to state a claim under either the NJIPPA or NCCIPA. Plaintiffs have not plausibly alleged a claim under either statute where they have only alleged that their personal information was stolen from Defendants, not that Defendants disclosed the data to the cyberattackers. Therefore, the Court grants the Excellus Defendants' motion to dismiss Plaintiffs' NJIPPA and NCCIPA claims with prejudice, and leave to replead these claims is denied as futile.

V. Damages

The Excellus Defendants argue that, "even assuming [P]laintiffs have standing and have otherwise stated a valid claim, their complaint should be dismissed under Rule 12(b)(6) for failure to allege cognizable damages proximately caused by the Excellus cyberattack." (Excellus Mot. at 24). Plaintiffs disagree. (Pl. Excellus Opp. at 26).

Plaintiffs and the Excellus Defendants dispute whether it is appropriate for the Excellus Defendants to challenge Plaintiffs' damages theories wholesale, rather than challenge Plaintiffs' damages theories under each claim that Plaintiffs have pleaded. (*See* Pl. Excellus Opp. at 27; Excellus Reply at 17). The Excellus Defendants contend that

“courts do not analyze these damages issues in a claim-specific manner.” (Excellus Reply at 17).

The Court is not convinced by the Excellus Defendants’ reply argument. The cases on which the Excellus Defendants rely—*Pisciotta*, 499 F.3d at 636-40, and *Hammond v. Bank of N.Y. Mellon Corp.*, 2010 WL 2643307, at *1-2 (S.D.N.Y. June 25, 2010)—do not support the proposition that “courts do not analyze these damages issues in a claim-specific manner.” In *Pisciotta*, 499 F.3d at 635, the Seventh Circuit considered “whether Indiana would consider that the harm caused by identity information exposure, coupled with the attendant costs to guard against identity theft, constitutes an existing compensable injury and consequent damages required to state a claim for negligence or for breach of contract” under the law of that state. Similarly, in *Hammond*, 2010 WL 2643307, at *9-13, the district court addressed the damages in the context of each of Plaintiffs’ claims under New York law.

Here, the Excellus Defendants make no attempt to identify whether Plaintiffs have sufficiently pleaded damages for purposes of each of their claims. Given that it is the movant’s burden to show why dismissal is warranted on a 12(b)(6) motion, the Court denies the Excellus Defendants’ motion, to the extent it is predicated on an alleged failure to plead any cognizable damages. *See Four K. Grp., Inc. v. NYCTL 2008-A Trust*, No. 12-CV-2135 (JG), 2013 WL 1562227, at *4 (E.D.N.Y. Apr. 15, 2013) (“[T]he movant bears the burden on a motion to dismiss under Fed. R. Civ. P. 12(b)(6).”); *see also In re Premiera Blue Cross Customer Data Sec. Breach Litig.*, No. 3:15-md-2633-SI, 2016 WL 4107717, at *17 (D. Or. Aug. 1, 2016) (“Whether that particular damage theory is sound

or whether that particular damages theory is state-specific are not issues that need to be resolved at this [motion-to-dismiss] stage of the litigation.”).

CONCLUSION

Based on the foregoing, the Excellus Defendants’ motion to dismiss for lack of standing (Dkt. 107) is granted with respect to the four non-misuse plaintiffs (Fero, Church, Boomershine, and Caltagarone). The claims by those plaintiffs are dismissed without prejudice. The Excellus Defendants’ motion to dismiss for lack of standing is in all other respects denied.

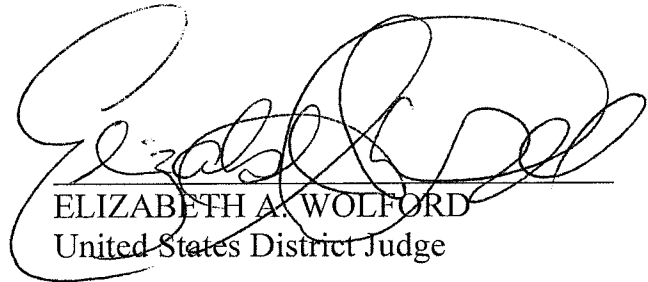
The Excellus Defendants’ motion to dismiss for failure to state a claim (Dkt. 107) is granted in part. Specifically, the motion is granted with respect to Plaintiffs’ (1) claim for breach of the implied covenant of good faith and fair dealing; (2) GBL § 349 claims, but only to the extent that those claims rest on paragraphs 281(d) and (e) of the CMC; (3) negligent misrepresentation claim; (4) CCRA claim; and (5) NJIPPA and NCCIPA claims. The Court dismisses those claims with prejudice, with the exception of Plaintiffs’ breach of the implied covenant of good faith and fair dealing claim, which may be pursued as part of Plaintiffs’ breach of contract claim, and Plaintiffs’ negligent misrepresentation claim, which Plaintiffs may attempt to replead. The Excellus Defendants’ motion to dismiss is otherwise denied.

BCBSA’s motion to dismiss for lack of standing (Dkt. 111) is denied. BCBSA’s motion to dismiss for failure to state a claim (Dkt. 111) is granted in part. Specifically, the motion is granted with respect to Plaintiffs’ (1) third-party beneficiary claim; and (2) request for benefit-of-the-bargain damages, and those claims are dismissed with

prejudice. Thus, the only surviving claim against BCBSA is Plaintiffs' GBL § 349 claim, to the extent it is not predicated on benefit-of-the-bargain damages.

In the event that Plaintiffs seek to attempt to file an amended complaint curing the deficiencies with respect to their negligent misrepresentation claim, they must do so within 20 days of the entry of this Decision and Order.

SO ORDERED.



ELIZABETH A. WOLFORD
United States District Judge

Dated: February 22, 2017
Rochester, New York